Basic Firewall Configuration

Version 1.2

Agenda

- Platform
- Ways to Manage
- Configuration Management
- Initial Configuration
- Interfaces
- Zones
- DHCP
- NAT
- Objects
- Licenses and Profiles
- Security Policies
- Routing
- Policy Based Forwarding
- USER-ID
- Troubleshooting
- Resources

Platform

Palo Alto Networks Portfolio coverage

Physical Firewalls

ML-Powered Next-Generation Firewall

App-ID | User-ID | Content-ID | Device-ID

Virtual Firewalls

Virtual Next-Generation Firewall

App-ID | User-ID | Content-ID | Device-ID

Containerized Firewalls

Containerized Next-Generation Firewall

App-ID | User-ID | Content-ID | Device-ID

Management tool

Firewall Management

Cloud based Secure access

Secure Access Service Edge

FWaaS | Secure Web Gateway | Zero Trust Network Access

Cloud Security

Cloud Native Security Platform

Protection | Cloud Network Security | Cloud Infrastructure

SD-WAN

Next-Generation SD-WAN

SD-WAN

Detect & Response / XDR

Extended Detection and Response

Endpoint Threat Prevention | Endpoint Detection & Response | Behavioral Analytics | Managed Detection & Response

SOC automation / XSOAR

Extended Security Orchestration, Automation and Response

Security Orchestration, Automation & Response | Threat Intelligence Management

Attack Surface Management / Xpanse

Attack Surface Management

Internet-Connected Asset Discovery & Mitigation

Unit 42 Security Consulting Services

Incident Response	Digital Forensics	Proactive Services	Exec & BoD Advisory	Cybersecurity Services
Ransomware | BEC | Cloud | APT | PCI	Forensics | Insider Threat | Expert Witness	Ransomware | BEC | Cyber Breach Assessments	vCISO | Program Design Strategy Review | M&A	Data Breach Response | Cyber Risk & Resilience Mgmt | Incident Response Services

Additional Services

Professional & Support Services
Resident Engineering | Professional Services | Focused Services

Cloud-Delivered Security Services

DNS Security	Threat Prevention	URL Filtering	WildFire	IoT Security	GlobalProtect	SD-WAN	Data Loss Prevention	Prisma SaaS
DNS Attack Prevention	Exploit, Malware, C2 Prevention	Malicious Site & Phishing Prevention	Malware Prevention	Enterprise IoT Security	Mobile User Security	Secure Branch Connectivity	Data Protection & Compliance	In-line & API SaaS Application Security

Platform Components

Panorama or Strata Cloud Manager

Security Subscriptions

ADV TP | ADV URL | WF | DNS | IoT | DLP | SaaS | GP | SD-WAN | AIOps

APP-ID | Content-ID | Device-ID | **PAN-OS** | User-ID | Cloud Identity | Decryption

Hardware	Software	Cloud Service
PA-Series	VM-Series / CN-Series	Prisma Access

Hardware: PA-Series

World's First Machine Learning-Powered Next Generation Firewall

PA-400 Series

PA-460
4.4 Gbps App-ID

PA-450
2.9 Gbps App-ID

PA-445
2.2 Gbps App-ID

PA-440
2.2 Gbps App-ID

PA-415
1.2 Gbps App-ID

PA-410
1.1 Gbps App-ID

PA-1400 Series

PA-1420
9.5 Gbps App-ID

PA-1410
6.8 Gbps App-ID

PA-3400 Series

PA-3440
24 Gbps App-ID

PA-3430
20.5 Gbps App-ID

PA-3420
16.9 Gbps App-ID

PA-3410
11 Gbps App-ID

PA-5400 Series

PA-5440
72 Gbps App-ID

PA-5430
61 Gbps App-ID

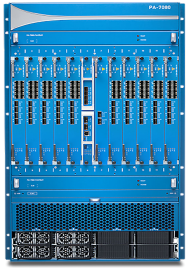
PA-5420
56 Gbps App-ID

PA-5410
43.5 Gbps App-ID

PA-5450

PA-5450
Up to 200 Gbps App-ID

PA-7000 Series



PA-7080
635 Gbps App-ID

PA-7050
384 Gbps App-ID

Small Branches — **Network Perimeter** — **Large Data Centers**

paloalto NETWORKS

Platform

Firewall Types

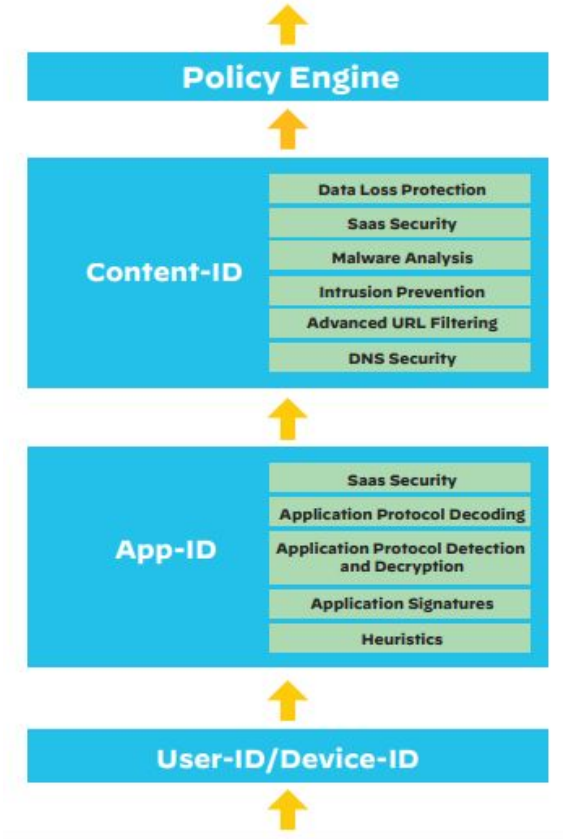
- Physical
  - Subscriptions (CDSS)/Bundles
    - Core Security Bundle
      - Advanced Threat Prevention
      - Advanced Wildfire
      - Advanced URL
      - DNS Security
      - Advanced SD-WAN
    - Globalprotect/Prisma Access Agent
  - Support
- Software (NGFW Credits)
  - On Premise
  - Cloud

Platform

Firewalls: Packet Flow

Single Pass Parallel Processing

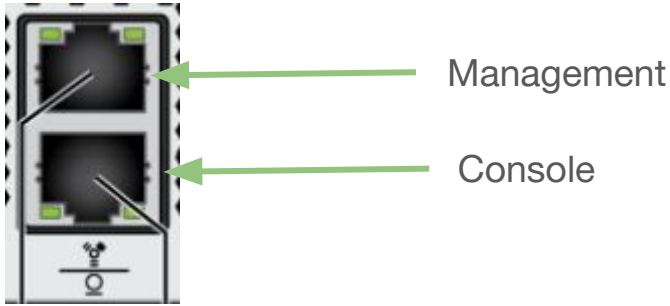
Packet Flow Processing



Ways to Manage

Ways to Manage

- Console
- CLI
- Web GUI
- API
- Panorama
- Strata Cloud Manager



Ways to Manage

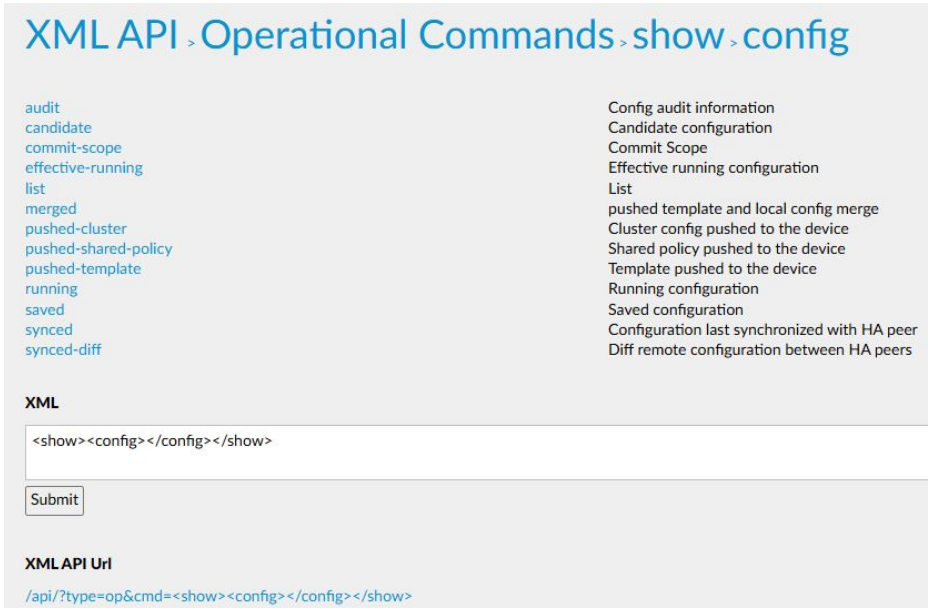
CLI:

```
admin@PA440-WAN> show interface management
  |        Pipe through a command
  <Enter>  Finish input

admin@PA440-WAN> show interface management


-------------------------------------------------------------------------------
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 1000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 8c:36:7a:02:c6:46

Ip address: 192.168.18.13
Netmask: 255.255.255.0
Default gateway: 192.168.18.1
Ipv6 address: unknown
Ipv6 link local address: fe80::8e36:7aff:fe02:c646/64
Ipv6 default gateway:
-------------------------------------------------------------------------------
```

Ways to Manage

XML-API:

- You can view the full list of resources in the REST API Reference on the firewall at https://<IP_address>/api



Ways to Manage

Rest-API:

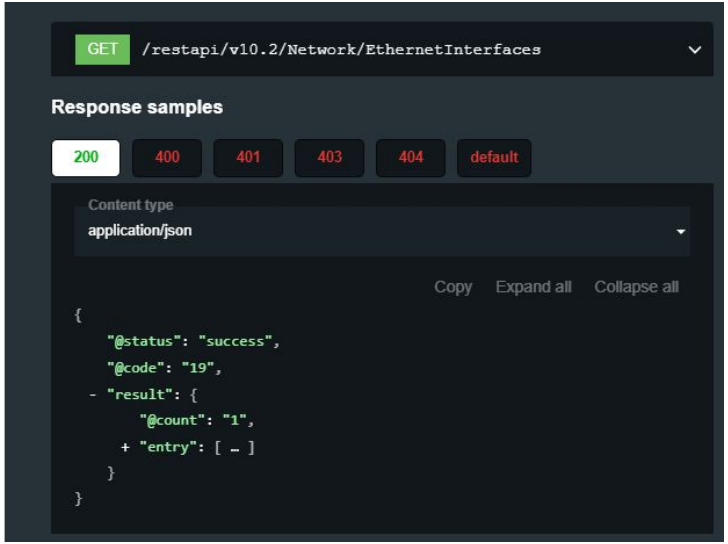
- You can view the full list of resources in the REST API Reference on the firewall at https://<IP_address>/restapi-doc.

List Ethernet Interfaces

Get Ethernet Interfaces.

QUERY PARAMETERS

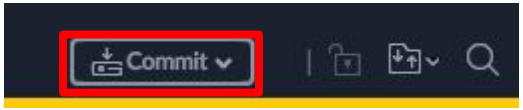
name	string The name of the entry
location	string Value: `"panorama-pushed"`
output-format	string Default: `"json"` Enum: `"json"` `"xml"` Specify the output format to be JSON or XML. This is equivalent to setting the `Accept` header to `application/json` or `application/xml`. If you include both `output-format` and `Accept` header, the value of `output-format` will override the header.

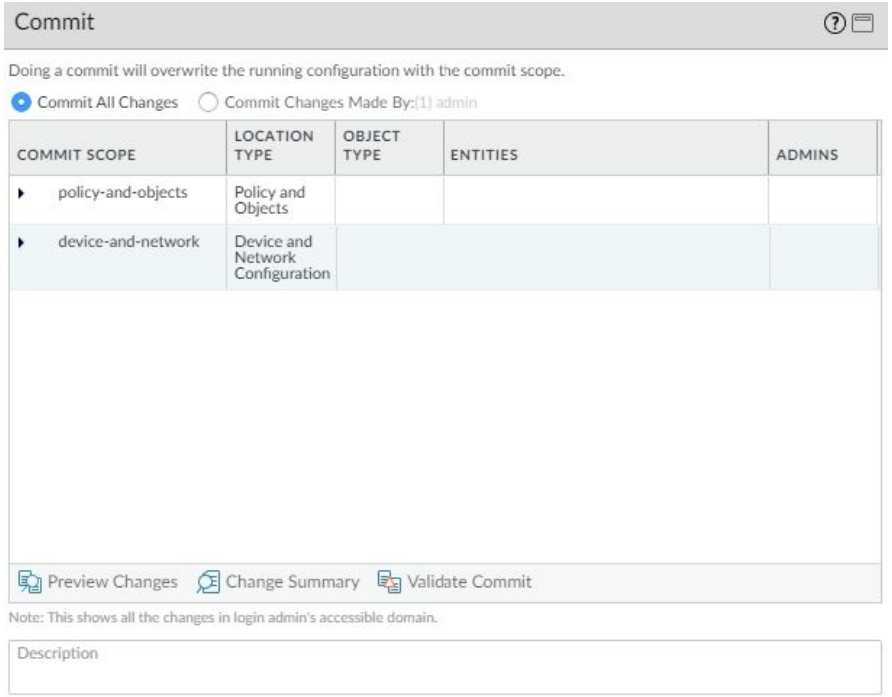


Configuration Management

Configuration Management

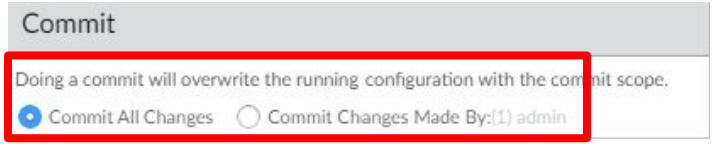
- Candidate Configuration - Configuration before a commit
- Running Configuration - Configuration after a commit





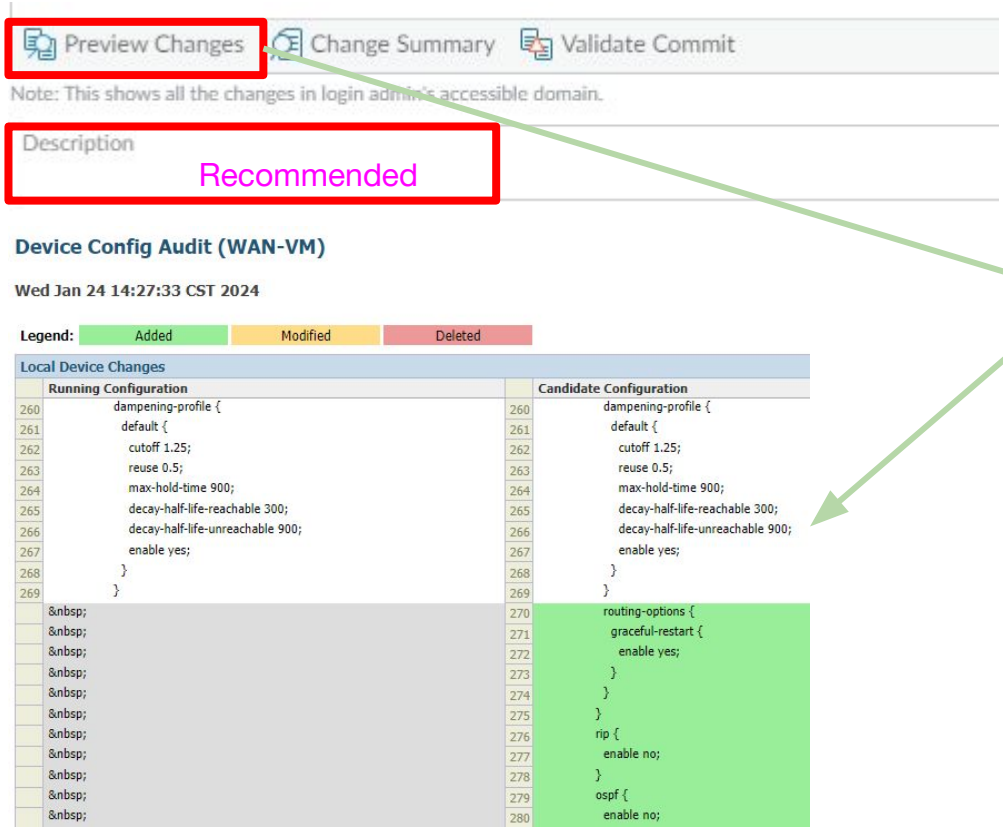
Configuration Management

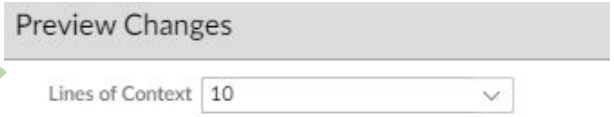
- Commit All Changes
- Commit Changes Made by current user



COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS
policy-and-objects	Policy and Objects			
outside		tag		admin
inside		tag		admin
Allowed URLs		Others		admin
default-1		Others		admin
dmz		tag		admin
Custom-URL-Profile		Others		admin
device-and-network	Device and Network Configuration			

Configuration Management

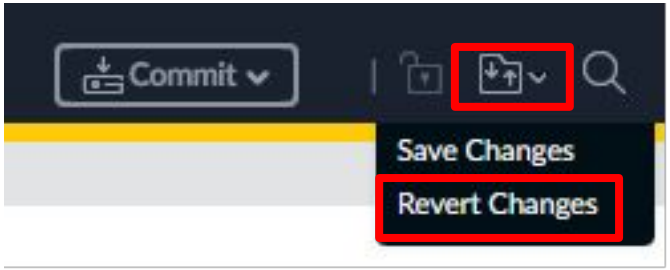




Configuration Management

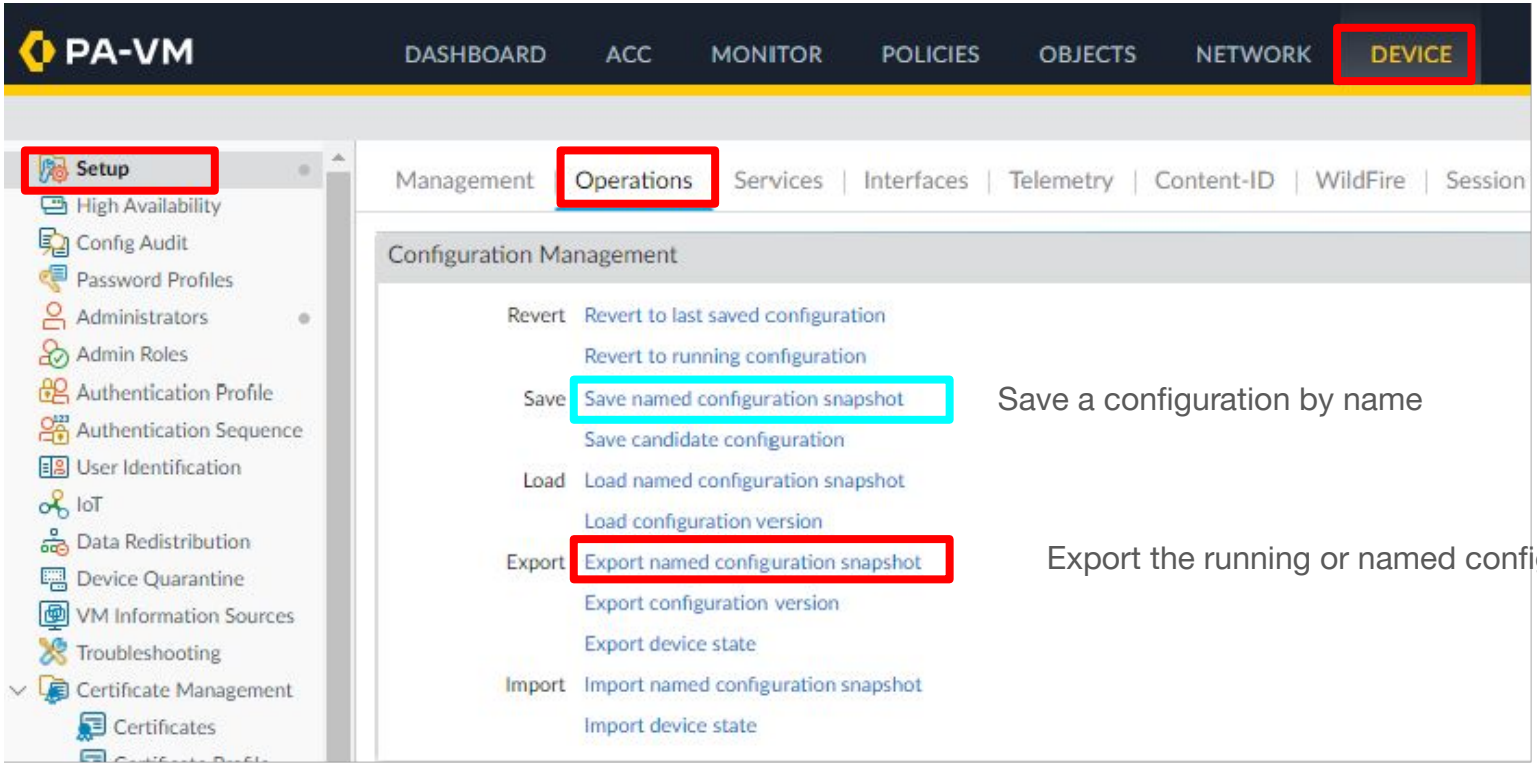
Revert candidate configuration changes:

- Remove changes made to the candidate configuration
- This is done before you commit changes



Configuration Management

Backing up a configuration:

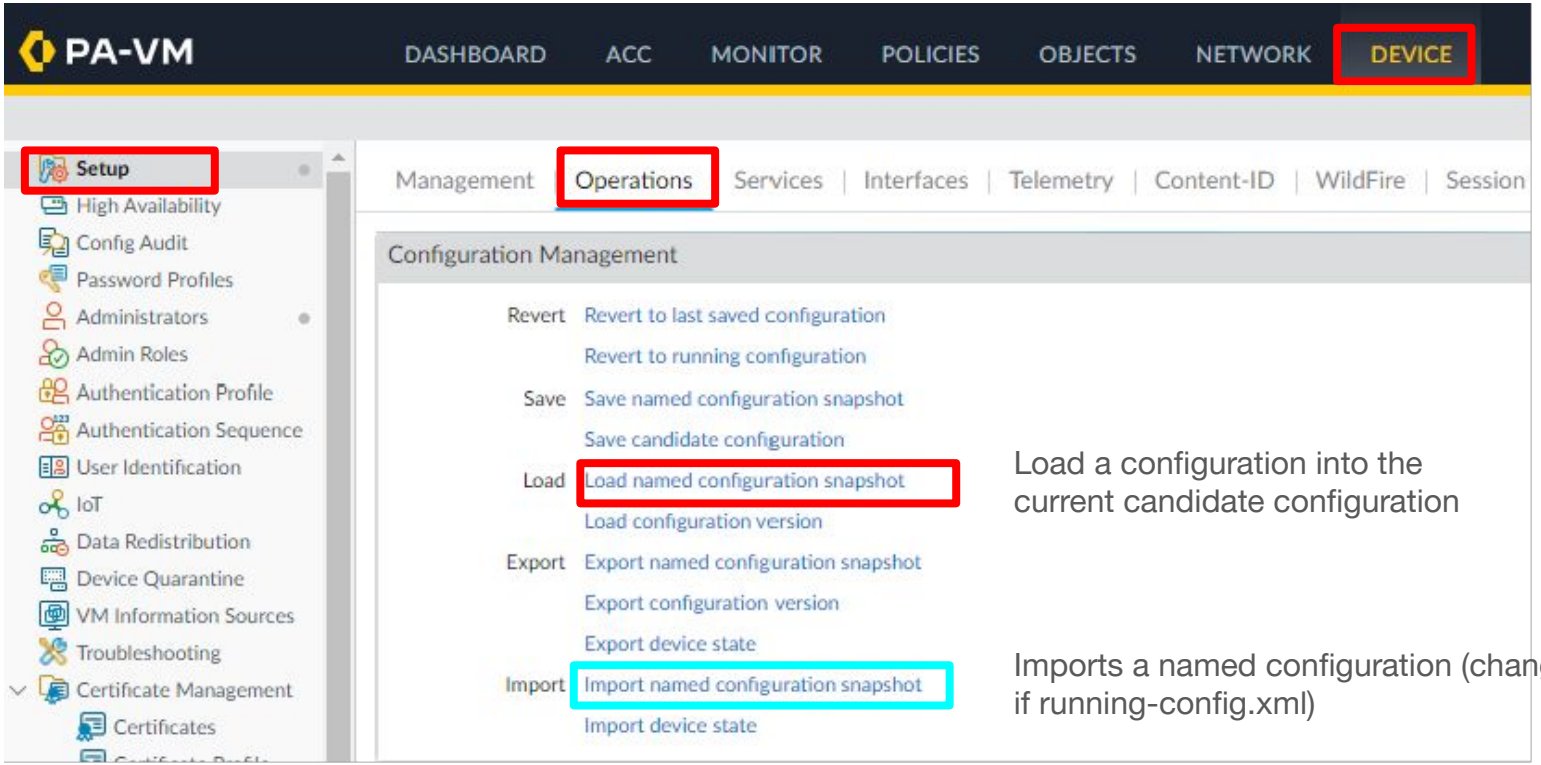


Save a configuration by name

Export the running or named configuration

Configuration Management

Restore a configuration:



Load a configuration into the current candidate configuration

Imports a named configuration (change name if running-config.xml)

Configuration Management

XML vs Set view:

- Exported configurations are in XML format
- XML Basics

- Set commands are used to configure a firewall via CLI or Console

View the configuration as a set command or XML format in the CLI or Console:

- "set" format: > set cli config-output-format set
- "xml" format: > set cli config-output-format xml

Configuration Management

XML Format (default)

```
admin@PA440-WAN# show
deviceconfig {
  system {
    hostname PA440-WAN;
    timezone US/Central;
    login-banner "You have accessed a protected system. Log off immediately if you are not an authorized user.";
    ntp-servers {
      primary-ntp-server {
        ntp-server-address 0.pool.ntp.org;
      }
      secondary-ntp-server {
        ntp-server-address 1.pool.ntp.org;
      }
    }
    snmp-setting {
      access-setting {
        version {
          v3;
        }
      }
    }
    update-schedule {
      threats {
        recurring {
          every-30-mins {
            at 2;
            action download-and-install;
```

Configuration Management

Set command format:

```
admin@PA440-WAN# show
set deviceconfig system hostname PA440-WAN
set deviceconfig system timezone US/Central
set deviceconfig system login-banner "You have accessed a protected system. Log off immediately if you are not an authorized user."
set deviceconfig system ntp-servers primary-ntp-server ntp-server-address 0.pool.ntp.org
set deviceconfig system ntp-servers secondary-ntp-server ntp-server-address 1.pool.ntp.org
set deviceconfig system snmp-setting access-setting version v3
set deviceconfig system update-schedule threats recurring every-30-mins at 2
set deviceconfig system update-schedule threats recurring every-30-mins action download-and-install
set deviceconfig system update-schedule threats recurring threshold 48
```

Initial Configuration

Initial Configuration

Management Interface Configuration:

- Default IP Address 192.168.1.1/24

Static IP Address

- Set new IP Address and Netmask
- Set Default-Gateway
- Set DNS Servers

DHCP IP Address

- Receive all information from a DHCP Server

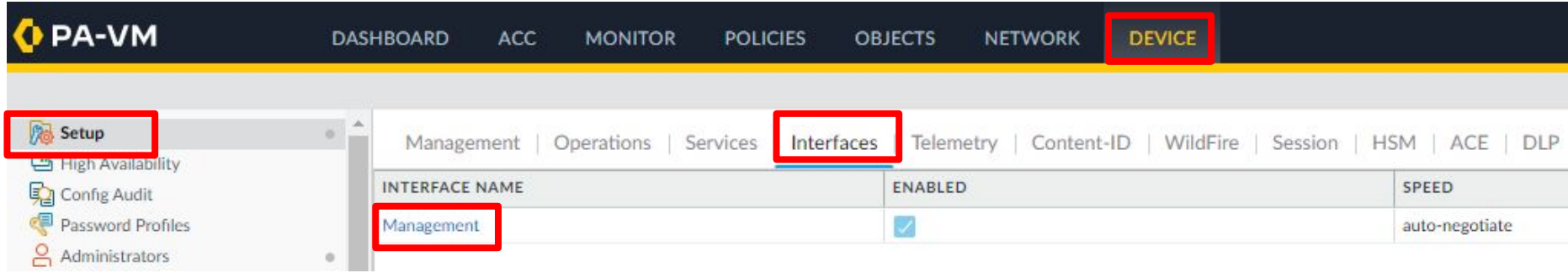
Initial Configuration

CLI Configuration for Static IP Address on Management Interface:

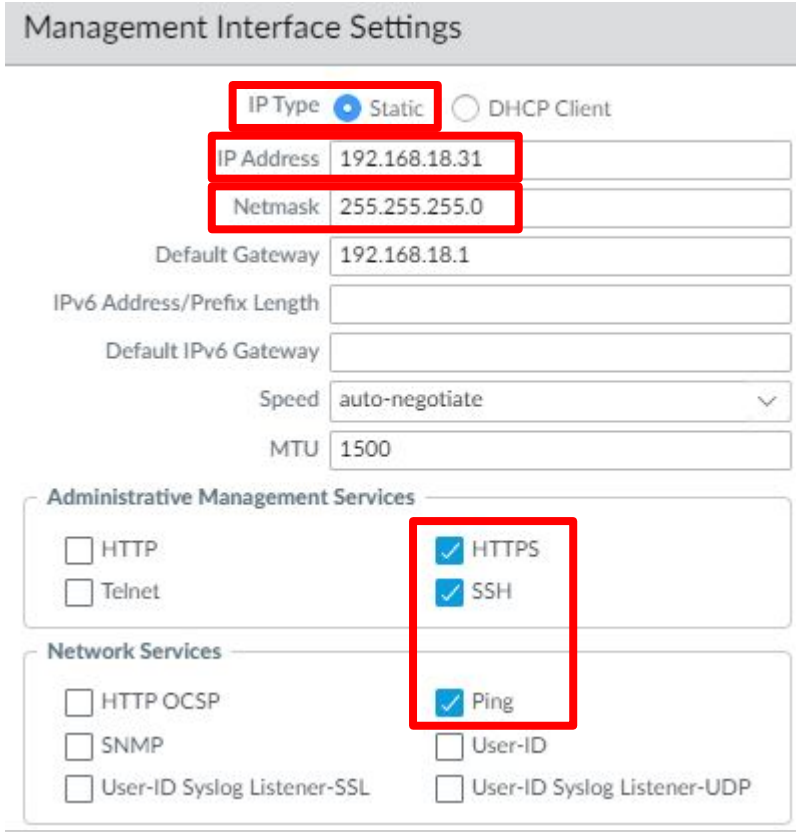
configure
set deviceconfig system type static
set deviceconfig system ip-address <IP_Address> netmask <Net_Mask>
set deviceconfig system default-gateway <Gateway>
set deviceconfig system dns-setting servers primary <dns-server>
set deviceconfig system dns-setting servers secondary <dns-server>
commit
exit

Initial Configuration

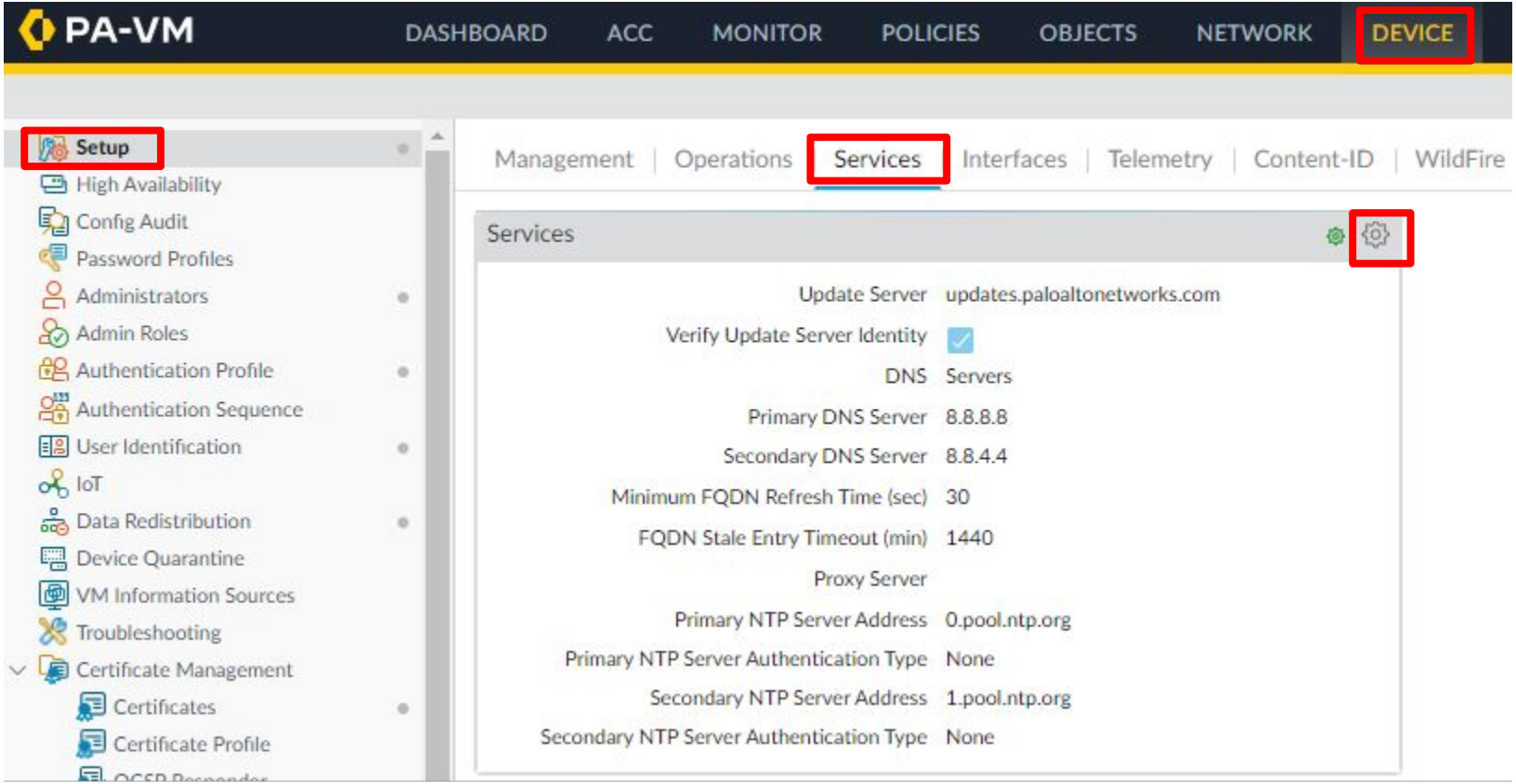
GUI Configuration for Management Interface:



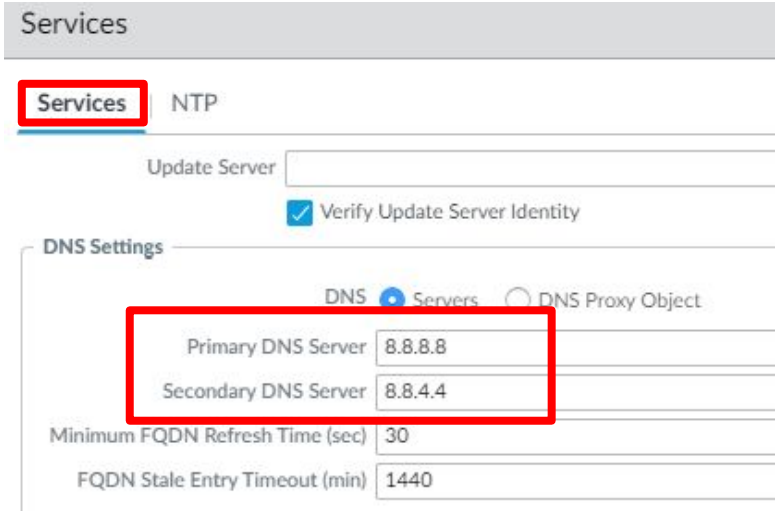
Initial Configuration

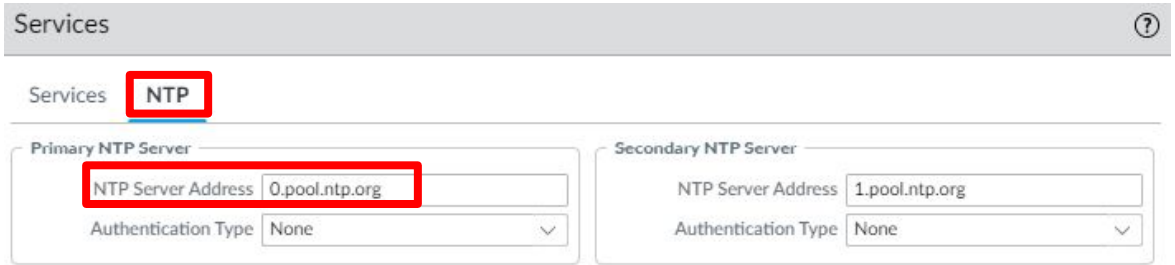


Initial Configuration



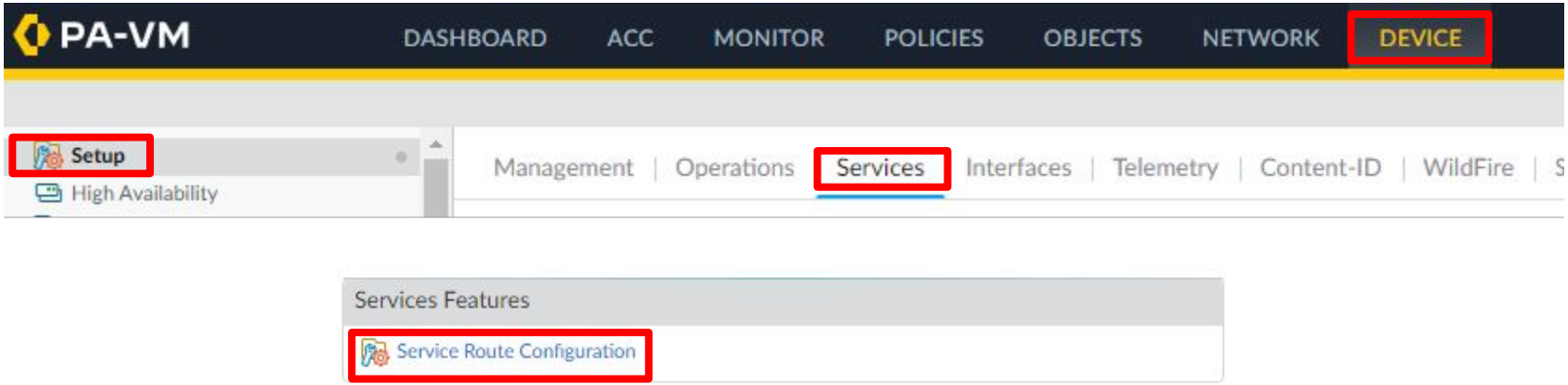
Initial Configuration



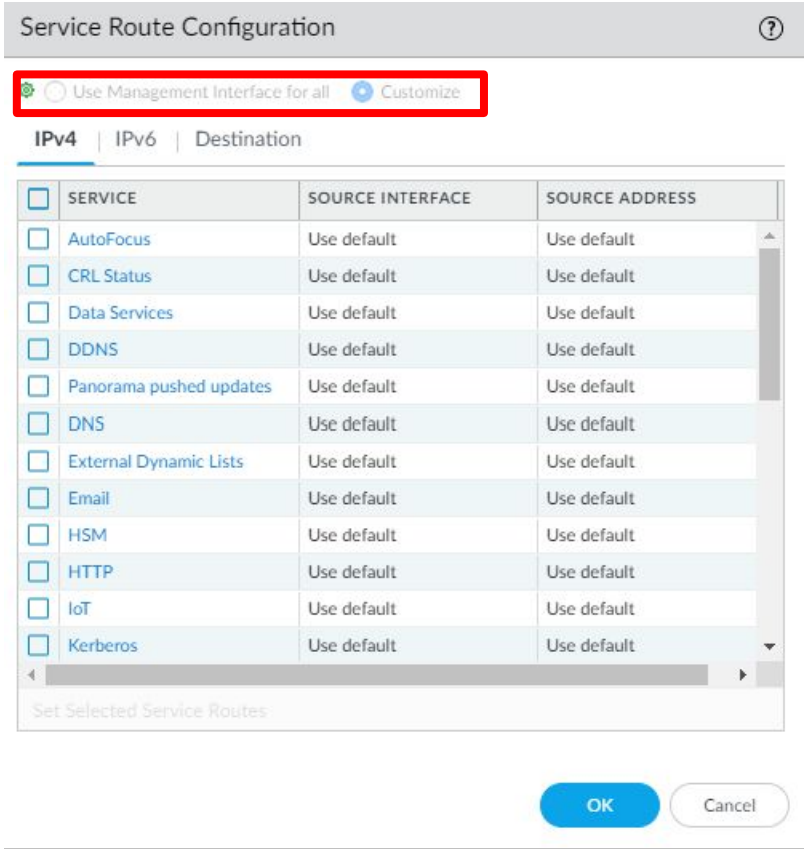


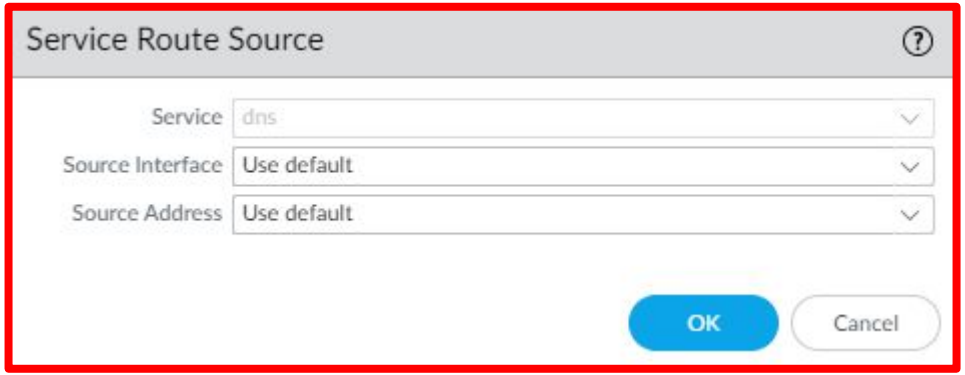
Initial Configuration

Service Routes:



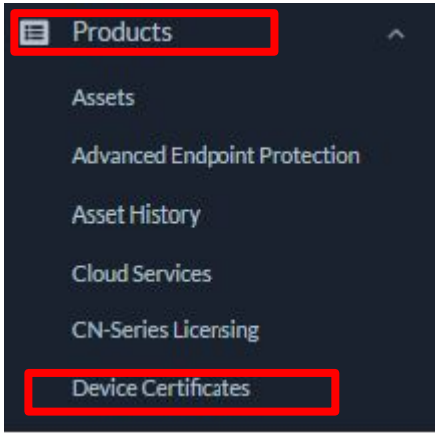
Initial Configuration

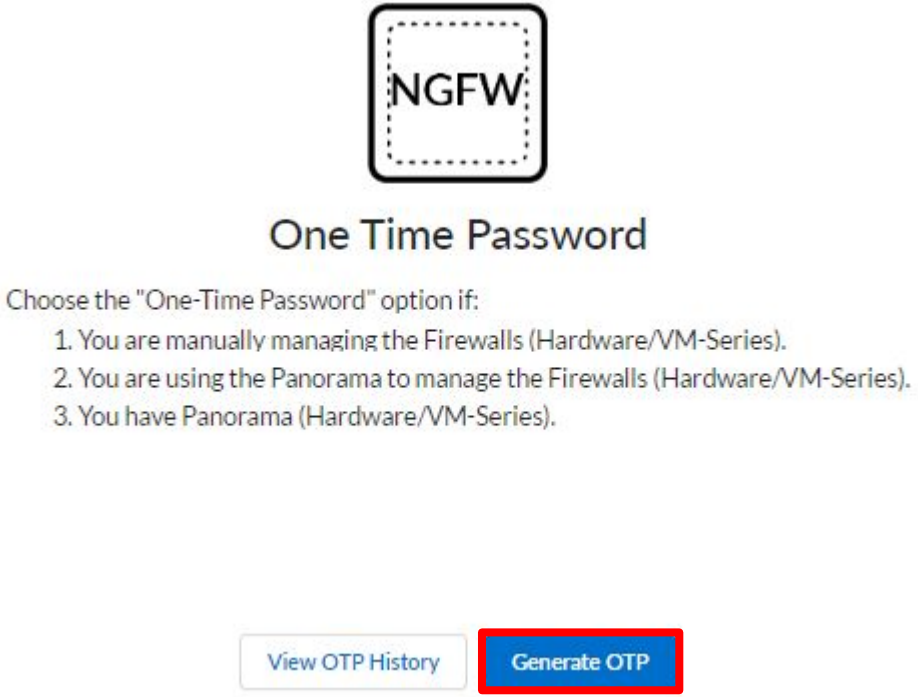




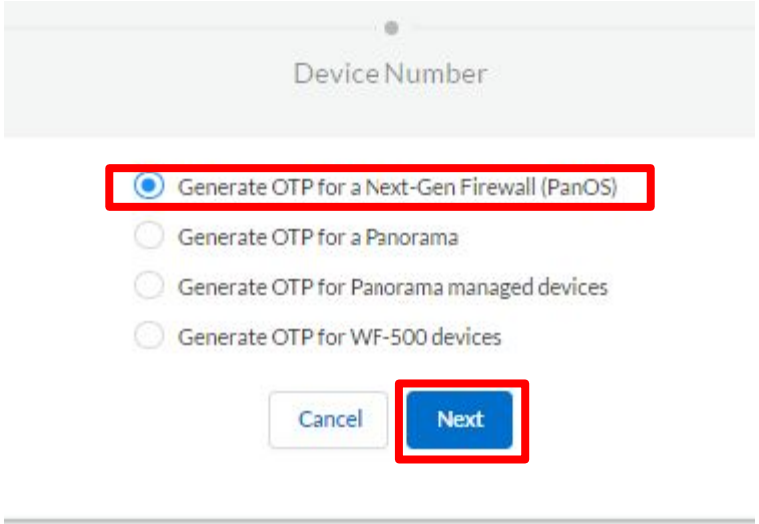
Initial Configuration

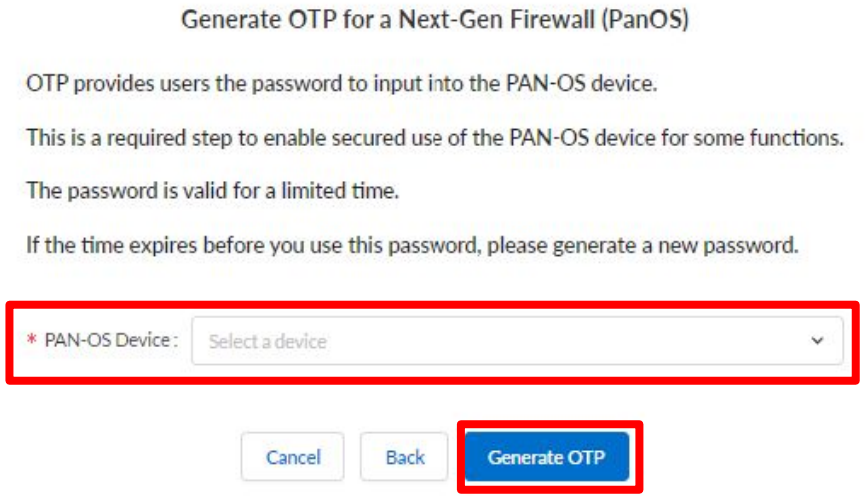
Device Certificate:



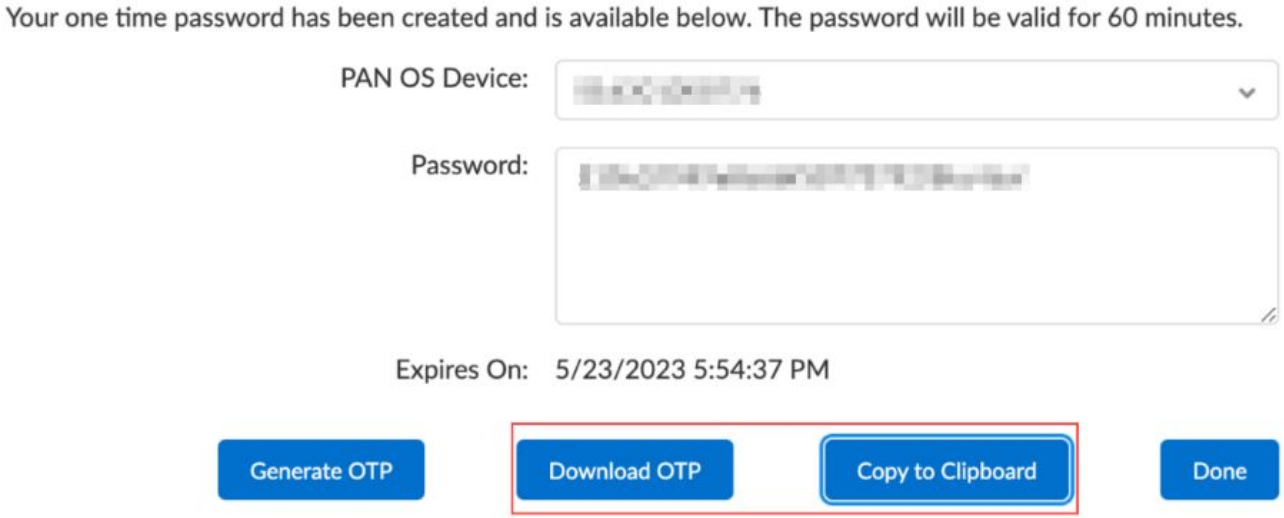


Initial Configuration





Initial Configuration

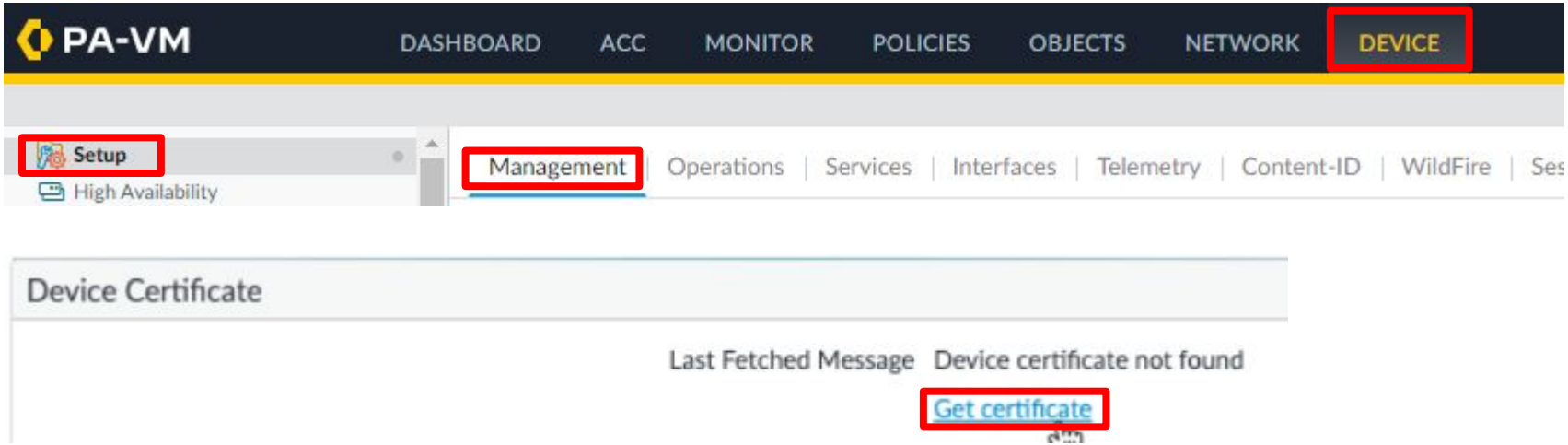


Initial Configuration

Import the OTP: CLI

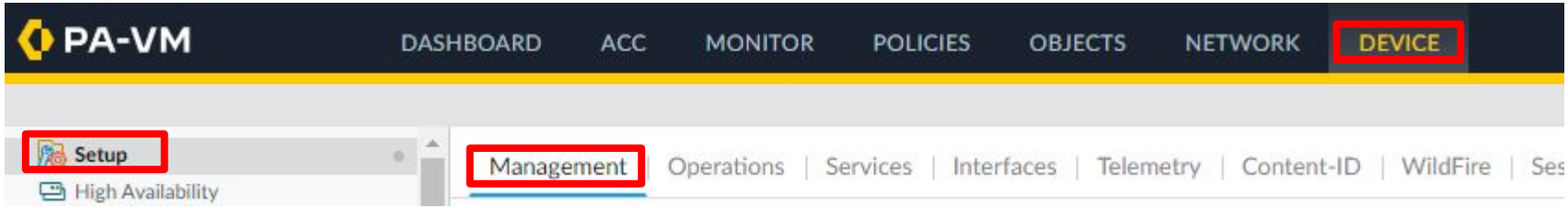
You can also install the device certificate from the firewall CLI using the command:

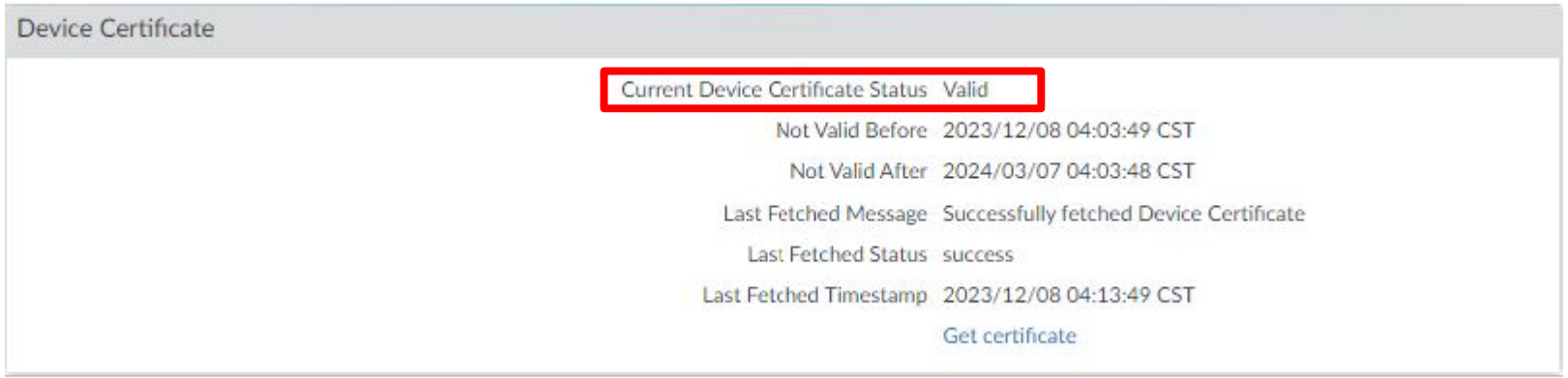
```
admin>request certificate fetch otp <otp_value>
```



Initial Configuration

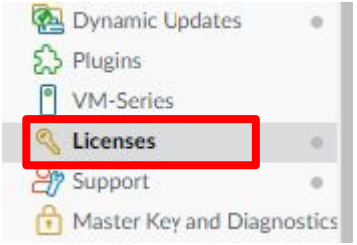
Device Certificate Validation:

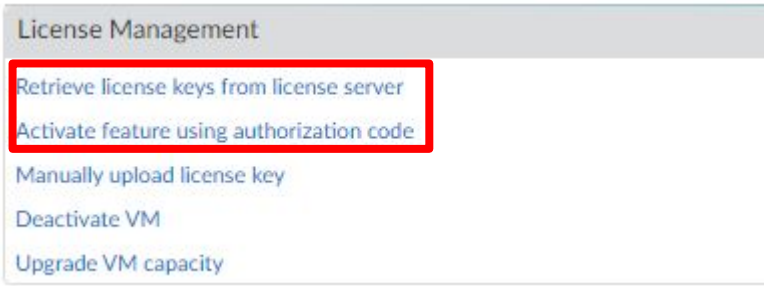




Initial Configuration

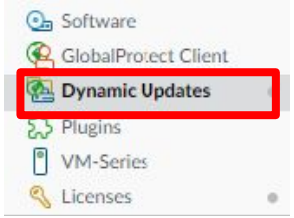
License the firewall: Device -> Licenses

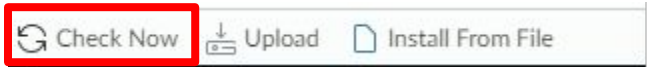




Initial Configuration

Dynamic Updates: Device -> Dynamic Updates



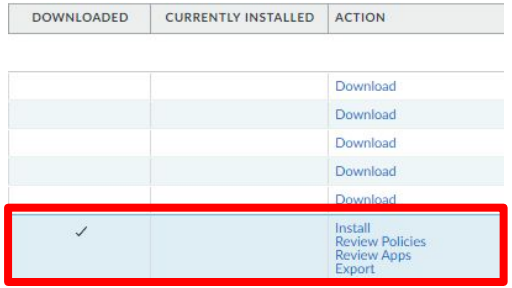


VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION
Applications and Threats	**Last checked:** 2024/01/16 17:04:06 CST	**Schedule:** Every Wednesday at 01:02 (Download only)							
8791-8464	panupv2-all-contents-8791-8464	Apps, Threats	Full	76 MB	e398e1db9b8729...	2023/12/18 15:25:59 CST			Download
8792-8469	panupv2-all-contents-8792-8469	Apps, Threats	Full	76 MB	d1469dd23f5408...	2023/12/19 16:38:55 CST			Download
8793-8478	panupv2-all-contents-8793-8478	Apps, Threats	Full	76 MB	bb01505fbcaaa9e...	2023/12/27 14:33:32 CST			Download
8795-8489	panupv2-all-contents-8795-8489	Apps, Threats	Full	76 MB	717744f8cd8feaa...	2024/01/08 12:26:00 CST			Download
8796-8491	panupv2-all-contents-8796-8491	Apps, Threats	Full	76 MB	917f47a2bda325...	2024/01/09 10:50:27 CST			Download
8797-8498	panupv2-all-contents-8797-8498	Apps, Threats	Full	77 MB	b996d57bf5d3c1...	2024/01/12 14:58:30 CST			Download
GlobalProtect Clientless VPN	**Last checked:** 2024/01/16 17:04:12 CST	**Schedule:** None							
98-260	panup-all-gp-98-260	GlobalProtectClientlessV...	Full	77 KB	52ef80beb11d00...	2023/05/22 17:41:22 CDT			Download
Device Dictionary	**Last checked:** 2024/01/16 17:04:08 CST								
107-458	panup-all-deviceid-107-458	IoT	Full	204 KB	ef96b8a528944f7...	2023/12/22 17:14:26 CST			
108-460	panup-all-deviceid-108-460	IoT	Full	204 KB	9f2fe8468061f71...	2023/12/29 13:37:56 CST			
109-462	panup-all-deviceid-109-462	IoT	Full	204 KB	91819e632a9396...	2024/01/04 16:31:12 CST			
110-464	panup-all-deviceid-110-464	IoT	Full	205 KB	301b6a5e18080c...	2024/01/11 10:28:40 CST			
WildFire	**Last checked:** 2024/01/16 17:04:11 CST	**Schedule:** None							
839107-842935	panupv3-all-wildfire-839107-842935	PAN OS 10.0 And Later	Full	8 MB	88544238792917...	2024/01/16 17:02:14 CST			Download

Initial Configuration

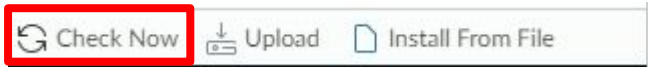
Dynamic Updates: Device -> Dynamic Updates

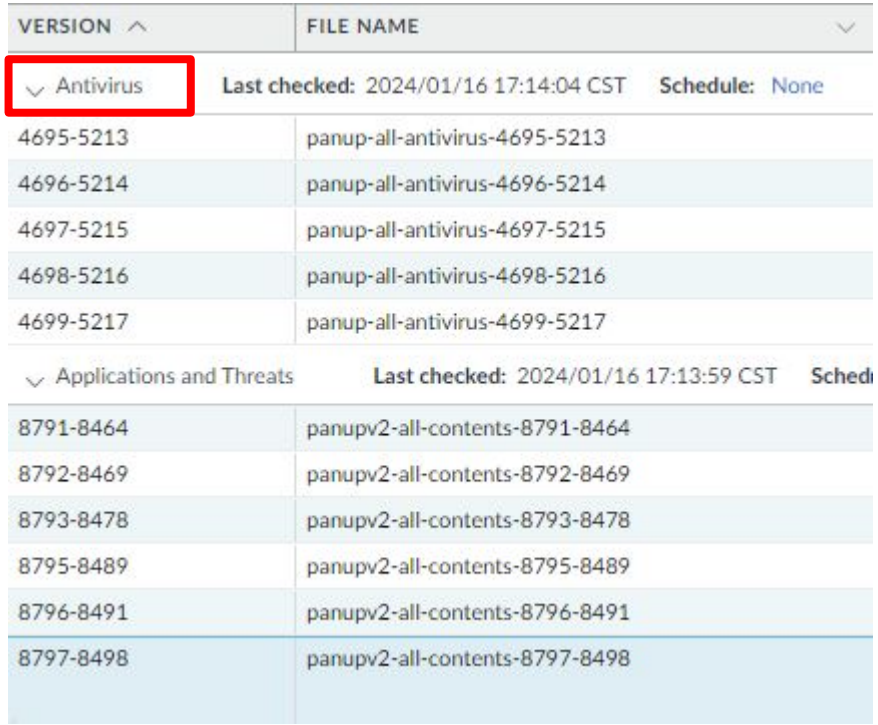
1.



2.

3.





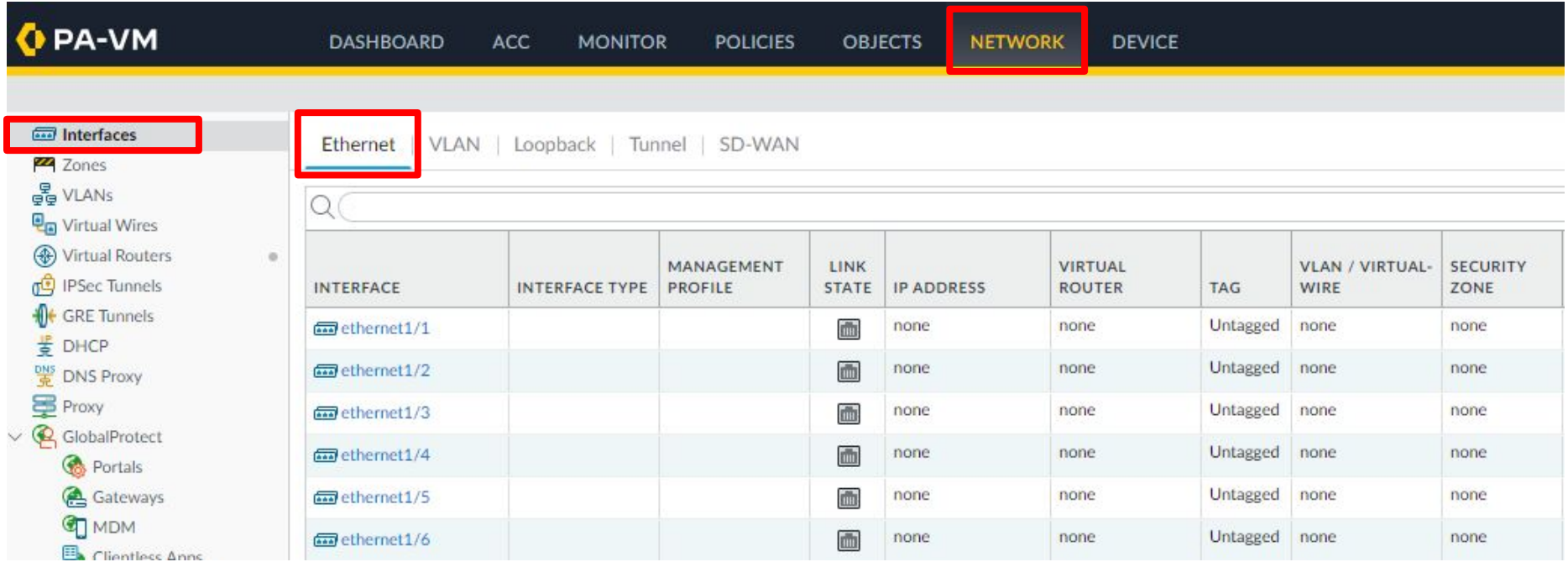
Interfaces

Interfaces

Interface Types:

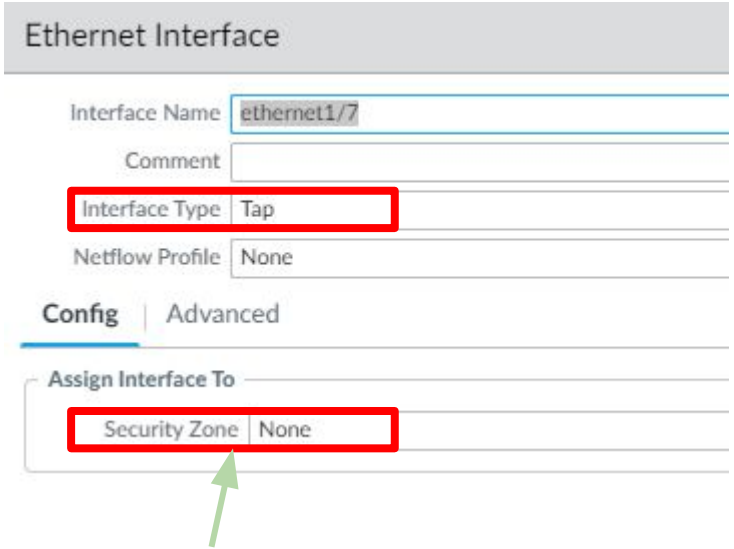
- Tap
- Virtual Wire
- Layer 2
- Layer 3
- Aggregate Ethernet
- HA
- Decrypt Mirror

Interfaces

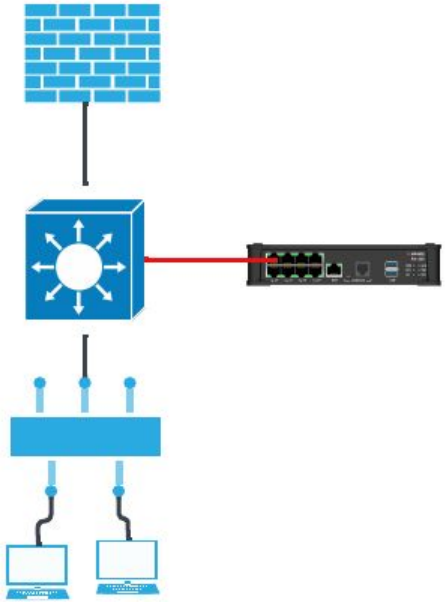


Interfaces

Tap Interface:

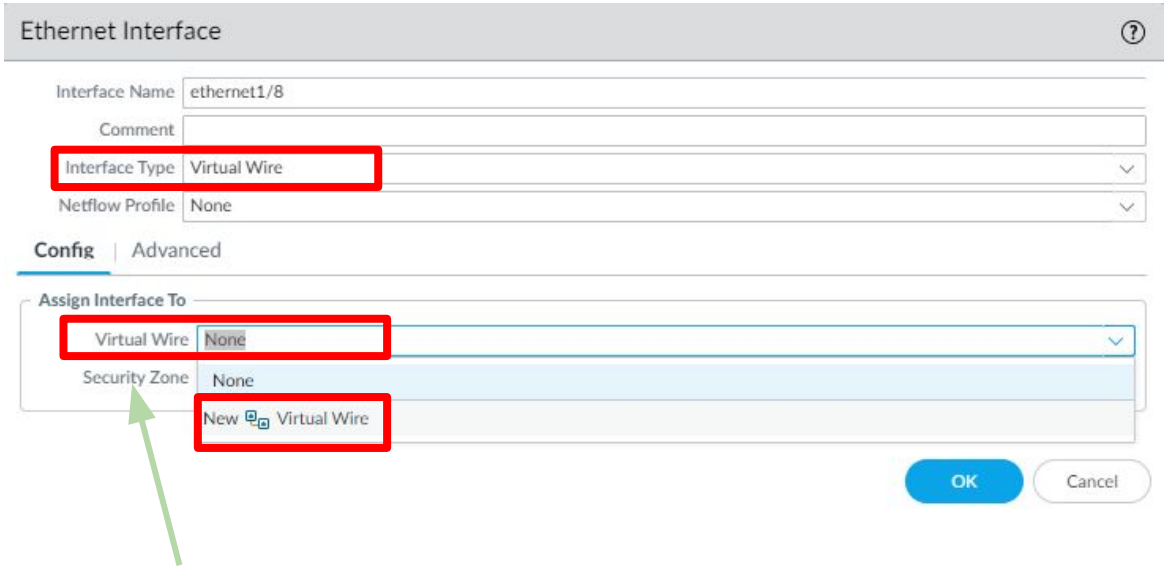


Add a Zone for the interface



Interfaces

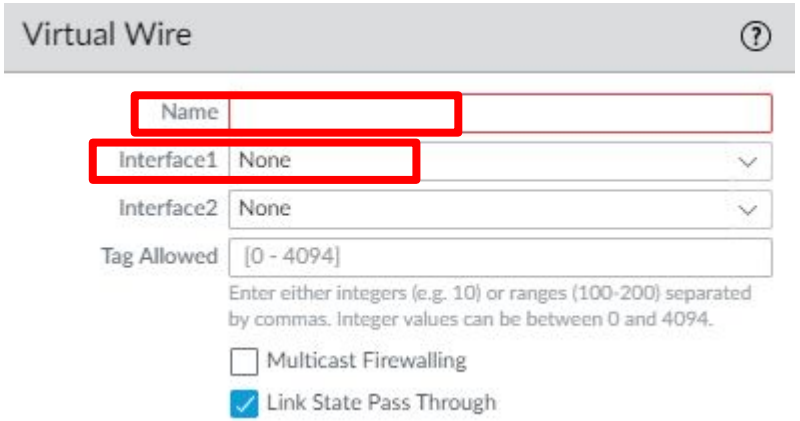
vWire Interface:



Add a Zone for the interface

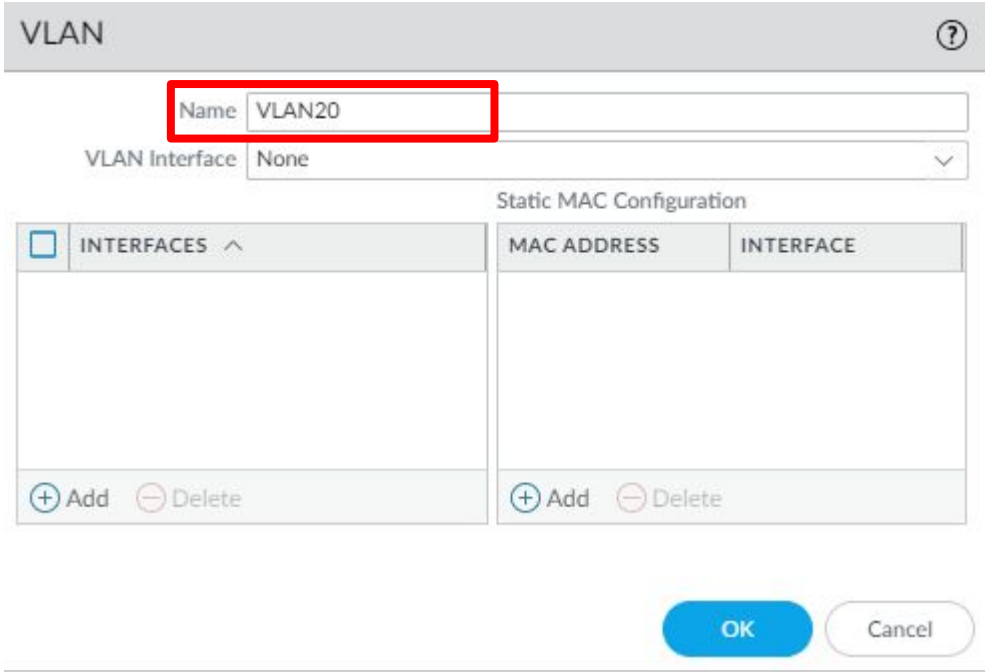
Interfaces

vWire Interface:



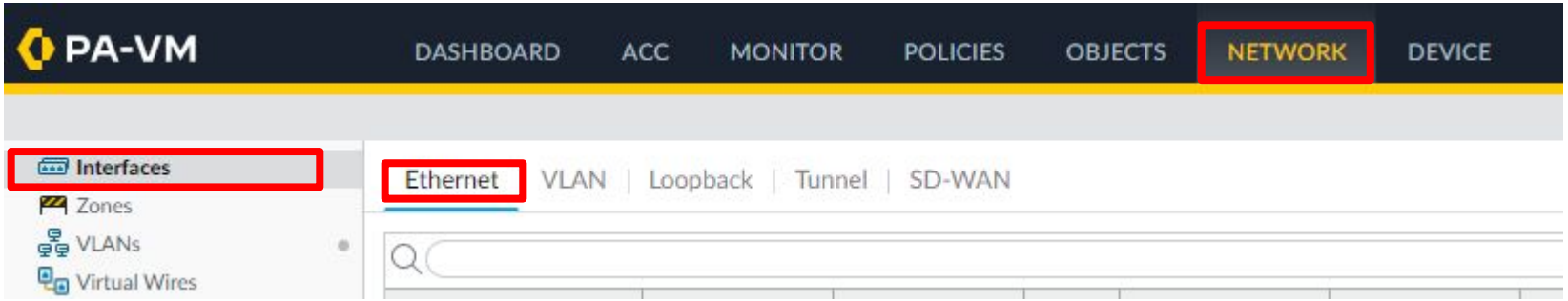
Interfaces

Layer 2 Interface: Create VLAN



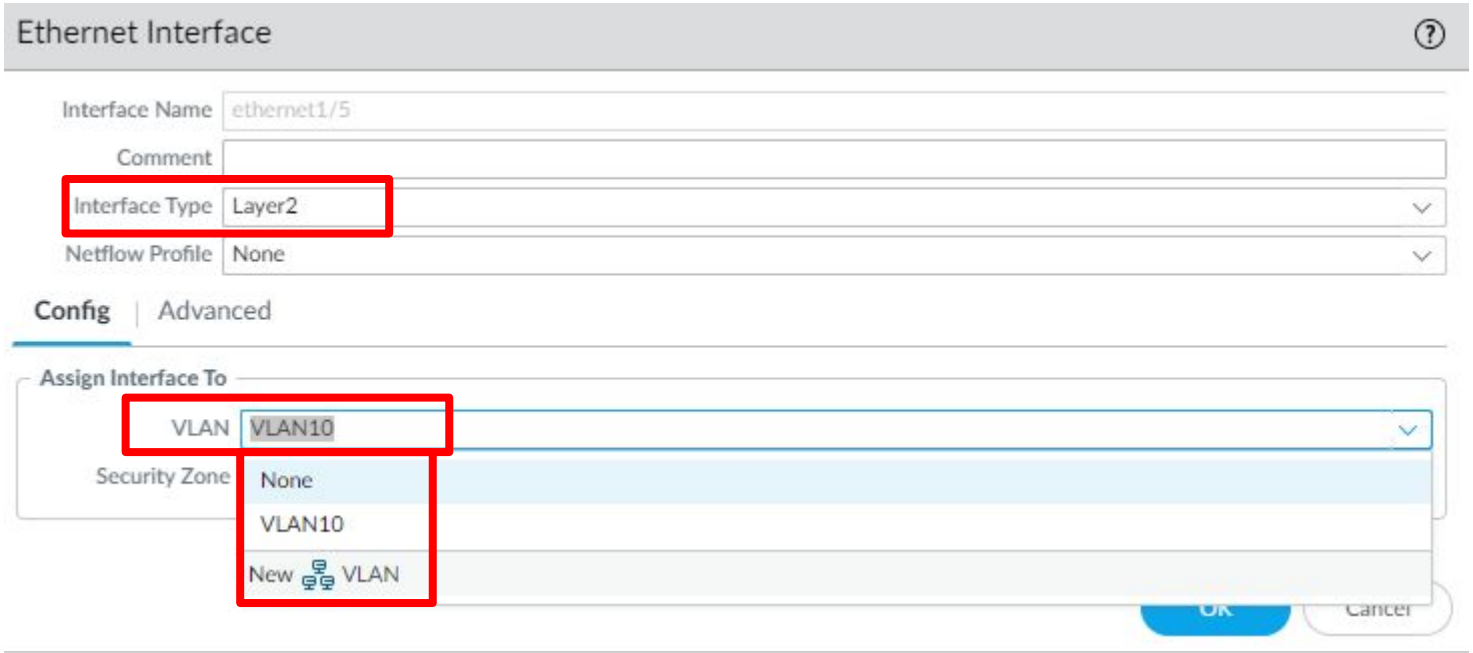
Interfaces

Layer 2 Interface:



Interfaces

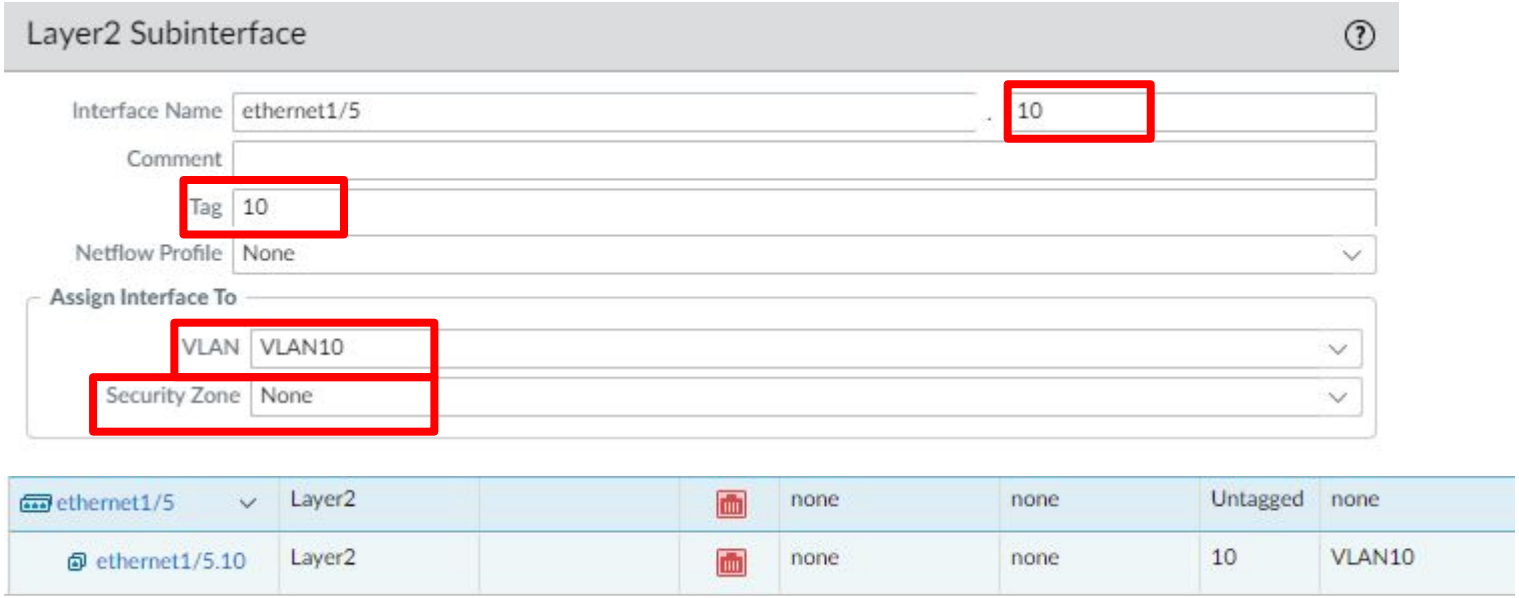
Layer 2 Interface: Single VLAN



Interfaces

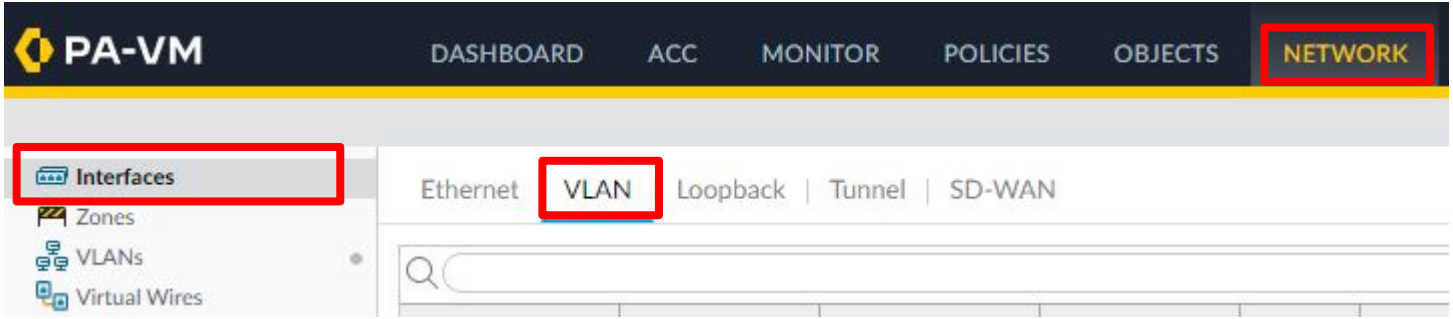
Layer 2 Interface: Multiple VLANs

Select the Interface and at the bottom of the page select: Add Subinterface



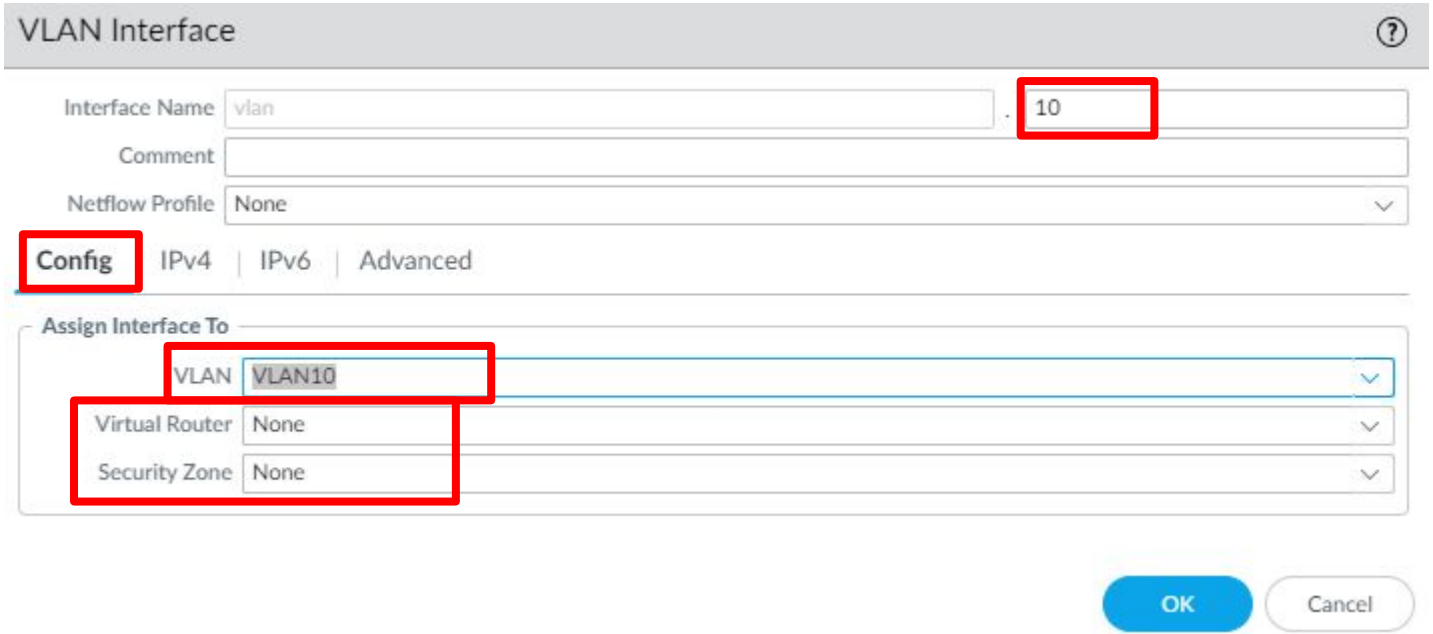
Interfaces

Layer 2 Interface: VLAN Interface



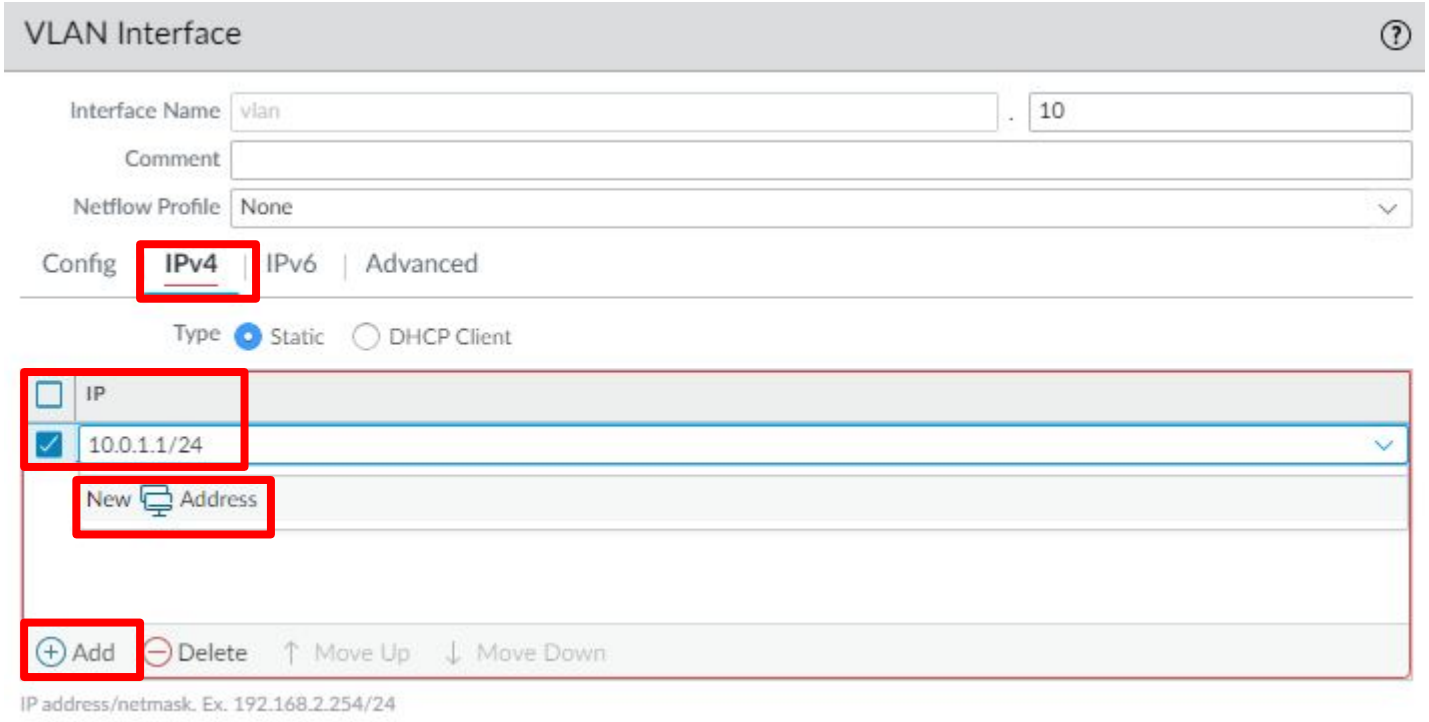
Interfaces

Layer 2 Interface: VLAN Interface



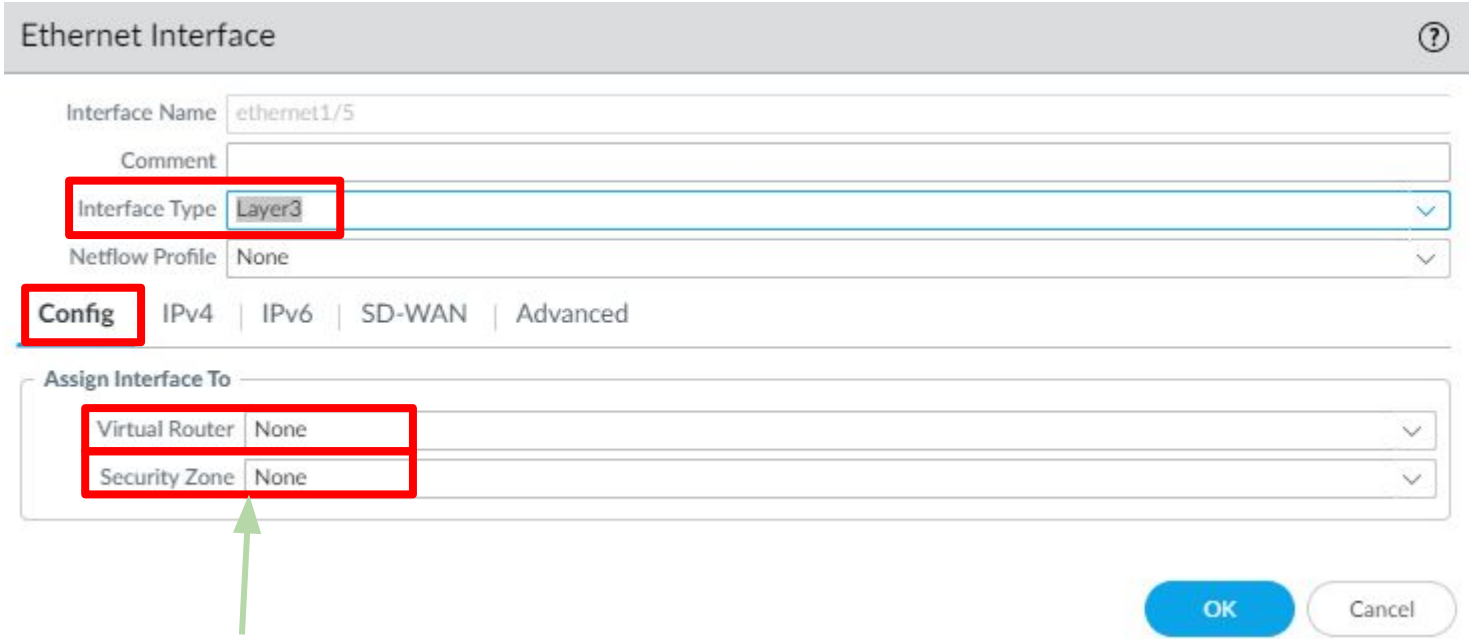
Interfaces

Layer 2 Interface: VLAN Interface



Interfaces

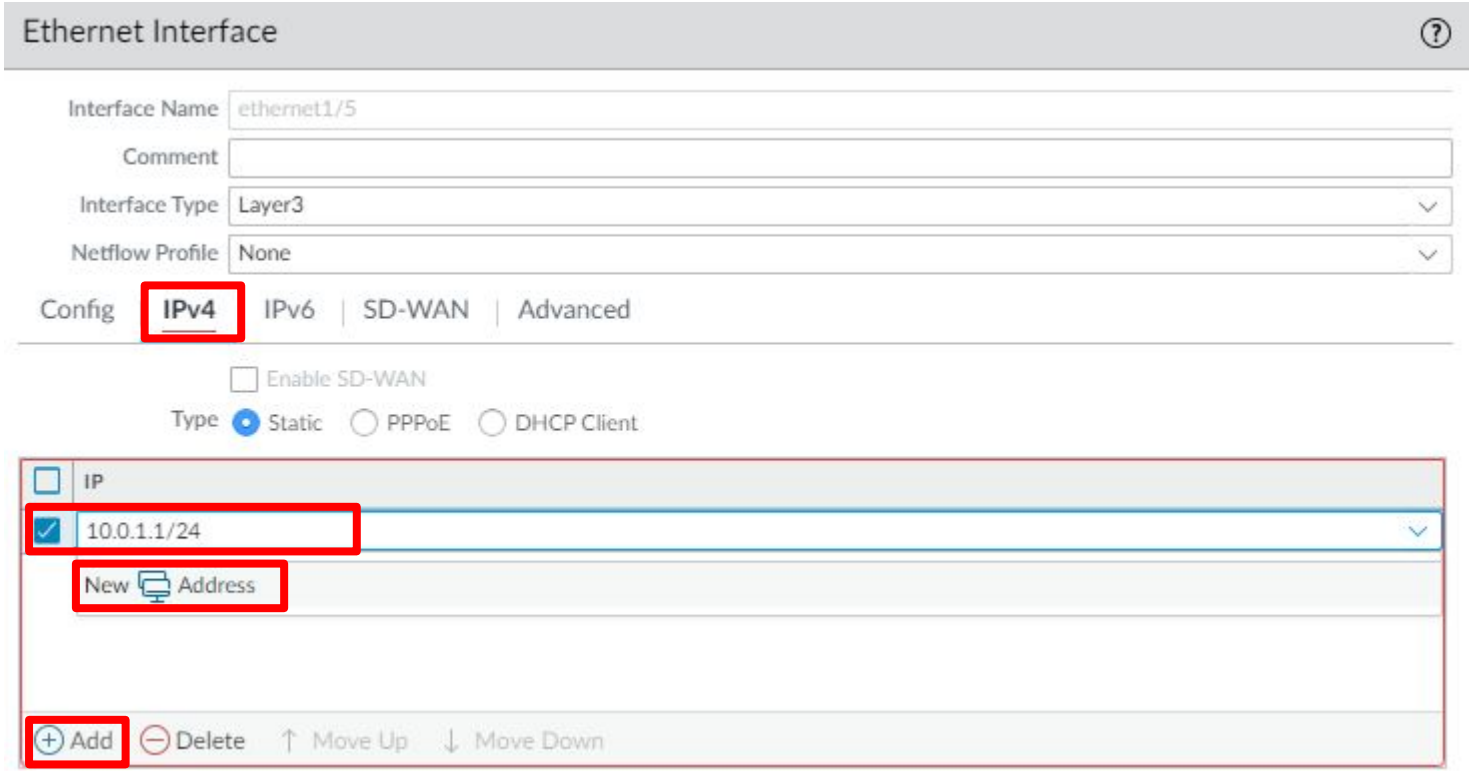
Layer 3 Interface:



Add a Zone and VR for the interface

Interfaces

Layer 3 Interface:



Interfaces

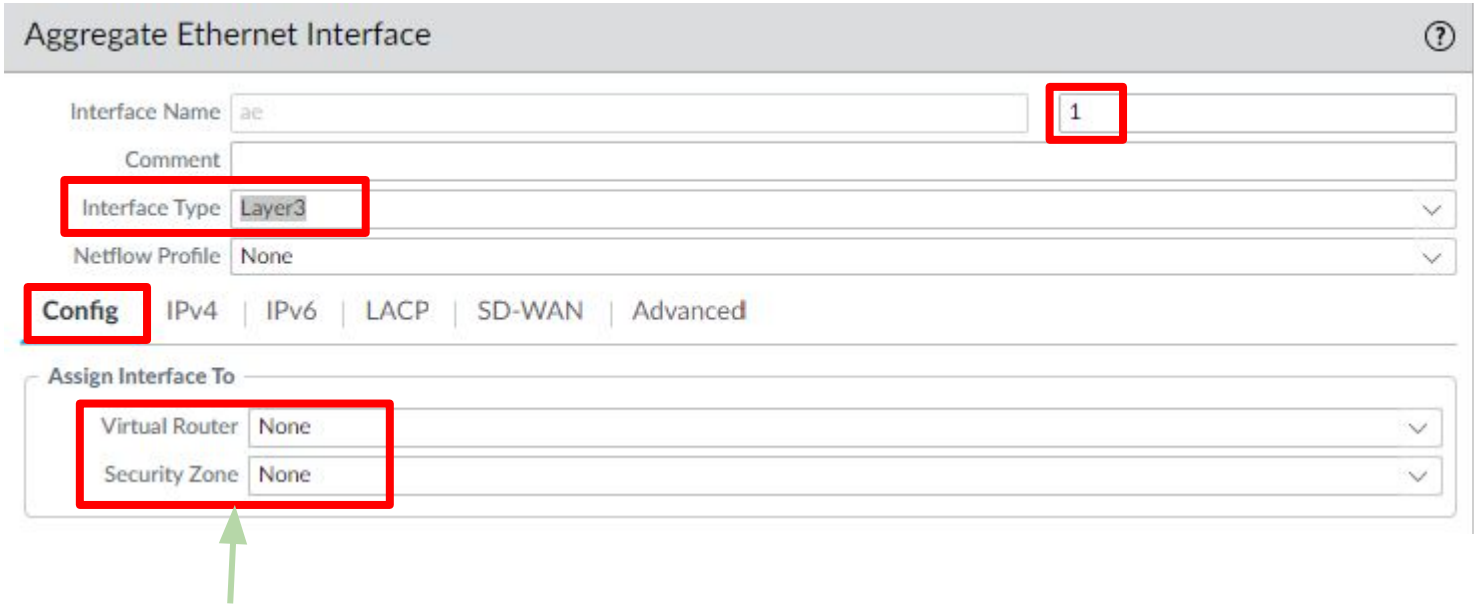
Port Aggregation:

Needs to be Physical hardware.

Select the interfaces you want to aggregate.

Interfaces

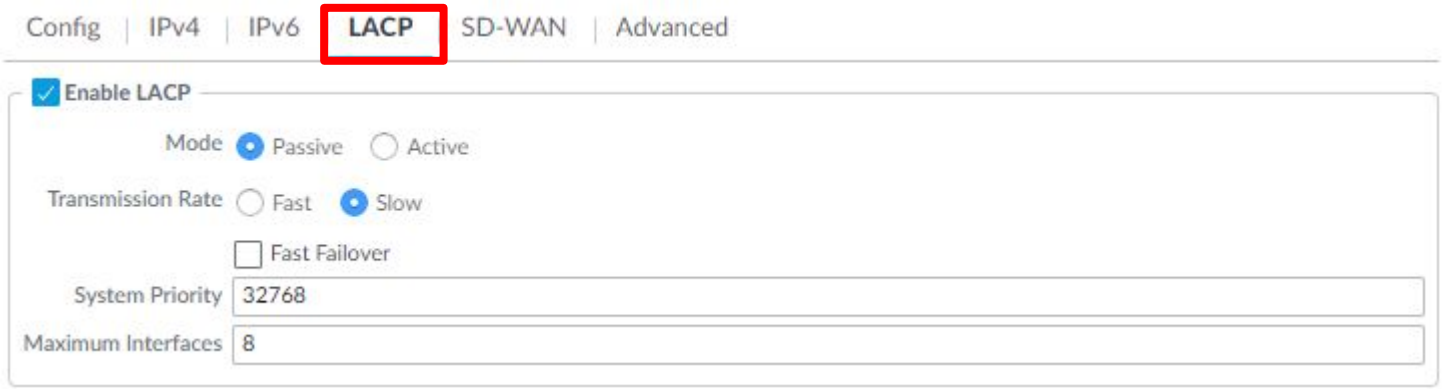
Port Aggregation:



Add a Zone and VR
for the interface

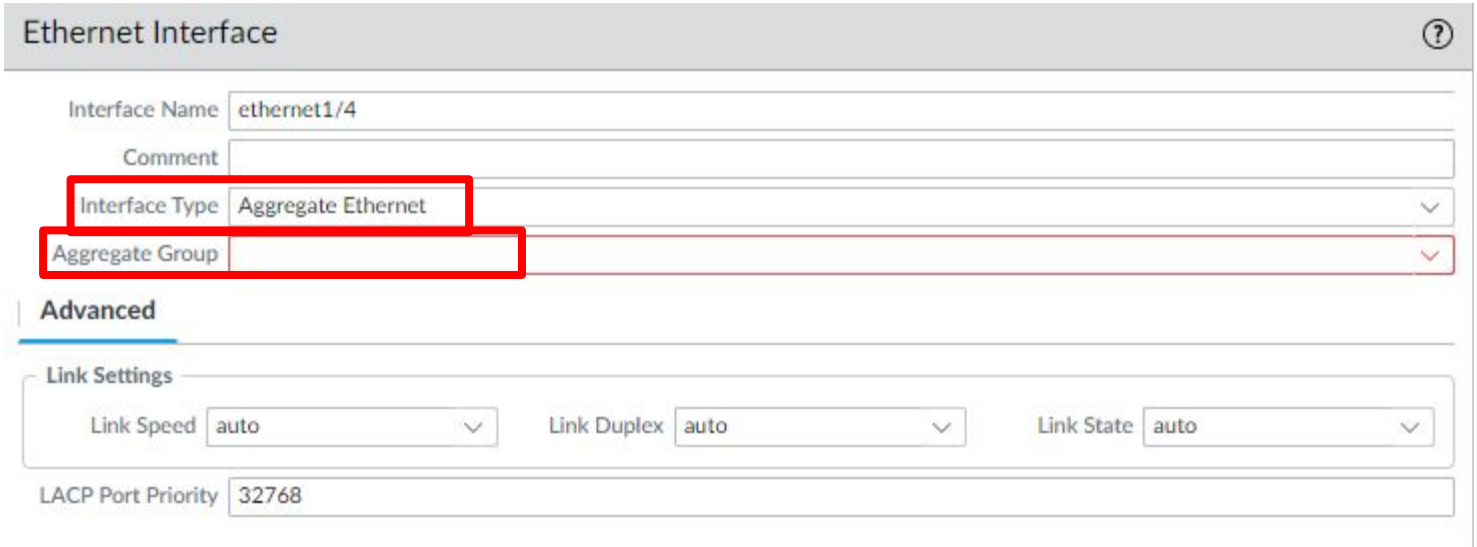
Interfaces

Port Aggregation:



Interfaces

Port Aggregation:



Interfaces

Interface Management Profiles:

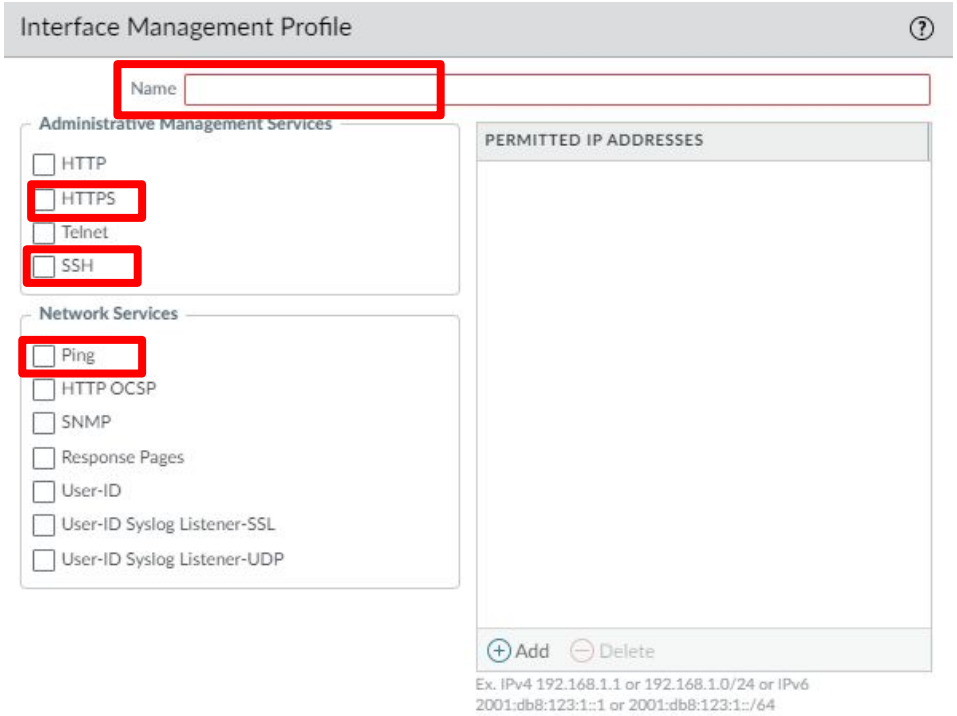
1. 

2. 

3. 

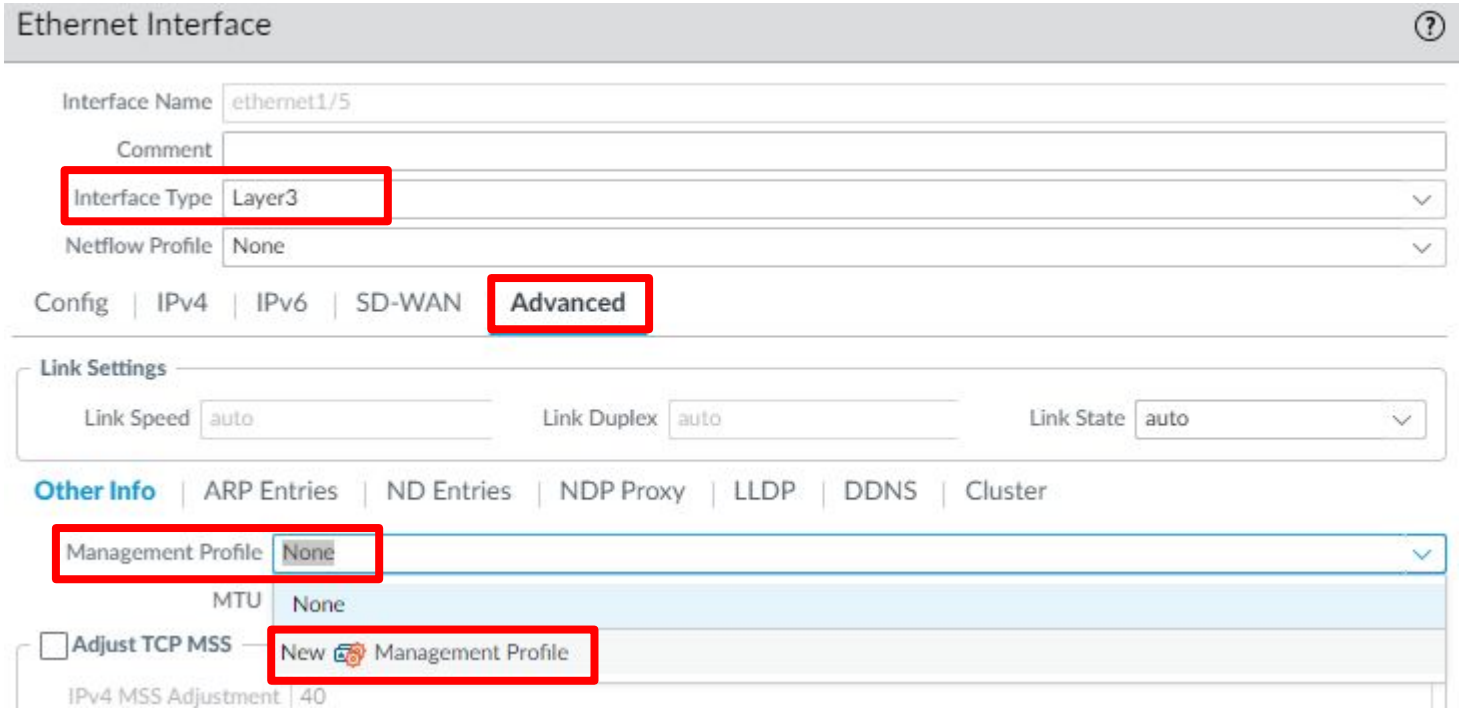
Interfaces

Interface Management Profiles:



Interfaces

Interface Management Profile: Apply to the Interface



Zones

Zones

Security zones are a logical way to group physical and virtual interfaces on the firewall to control and log the traffic that traverses specific interfaces on your network. An interface on the firewall must be assigned to a security zone before the interface can process traffic. A zone can have multiple interfaces of the same type assigned to it (such as tap, layer 2, or layer 3 interfaces), but an interface can belong to only one zone.

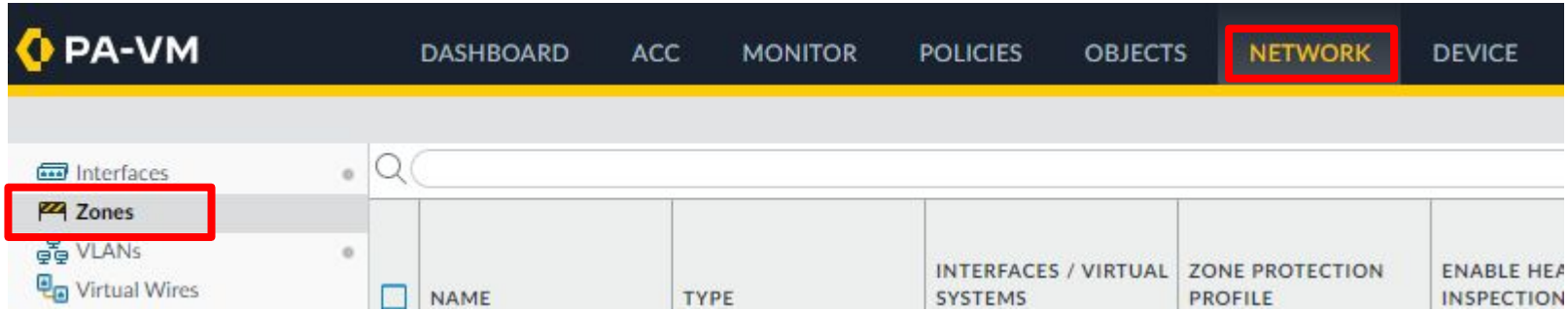
Policy rules on the firewall use security zones to identify where the traffic comes from and where it is going. Traffic can flow freely within a zone but traffic cannot flow between different zones until you define a Security policy rule that allows it. To allow or deny inter-zone traffic, Security policy rules must reference a source zone and destination zone (not interfaces) and the zones must be of the same type; that is, a Security policy rule can allow or deny traffic from one Layer 2 zone only to another Layer 2 zone.

Intrazone - Same Zone

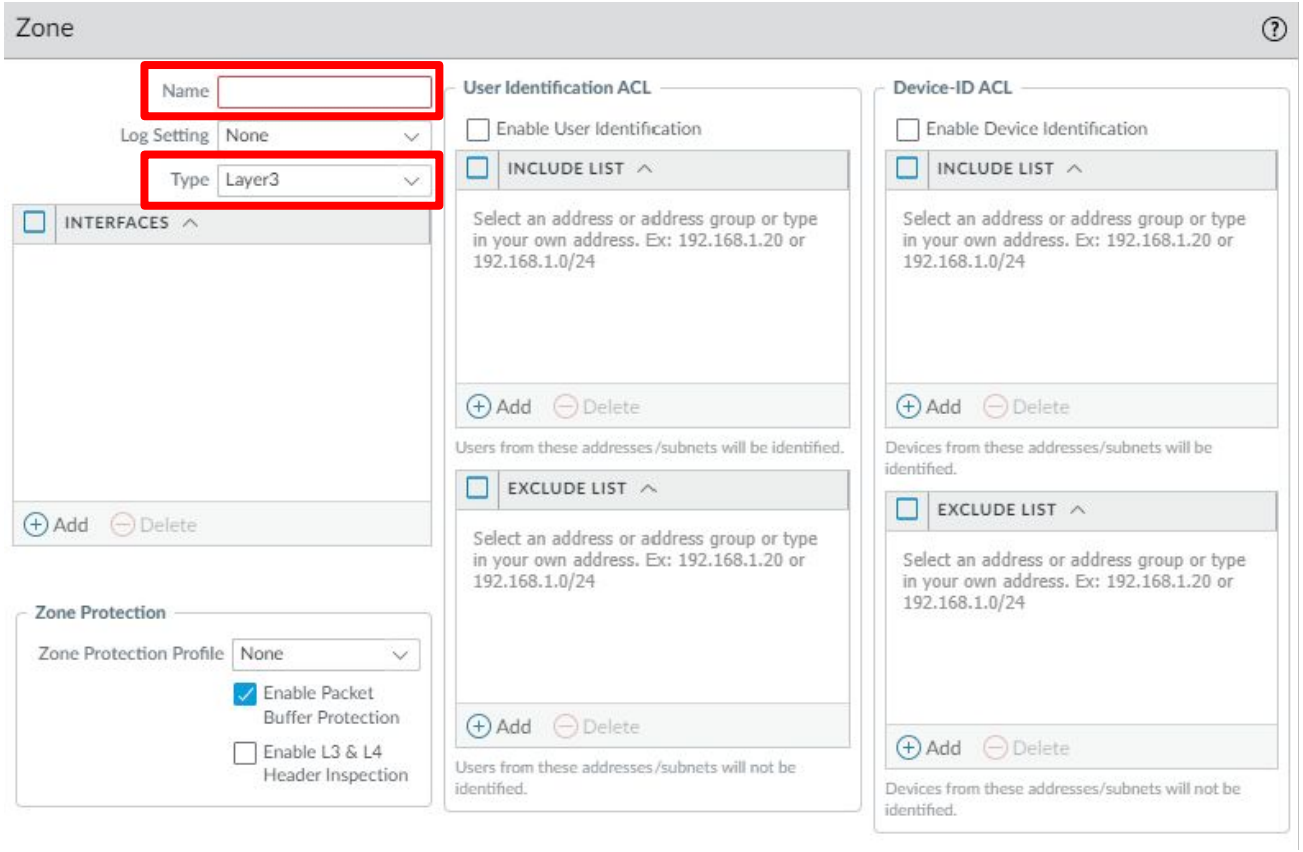
Interzone - Different Zone

Zones

Zones need to match the interfaces they are protecting. (i.e. L3 Zone -> L3 Interface)



Zones

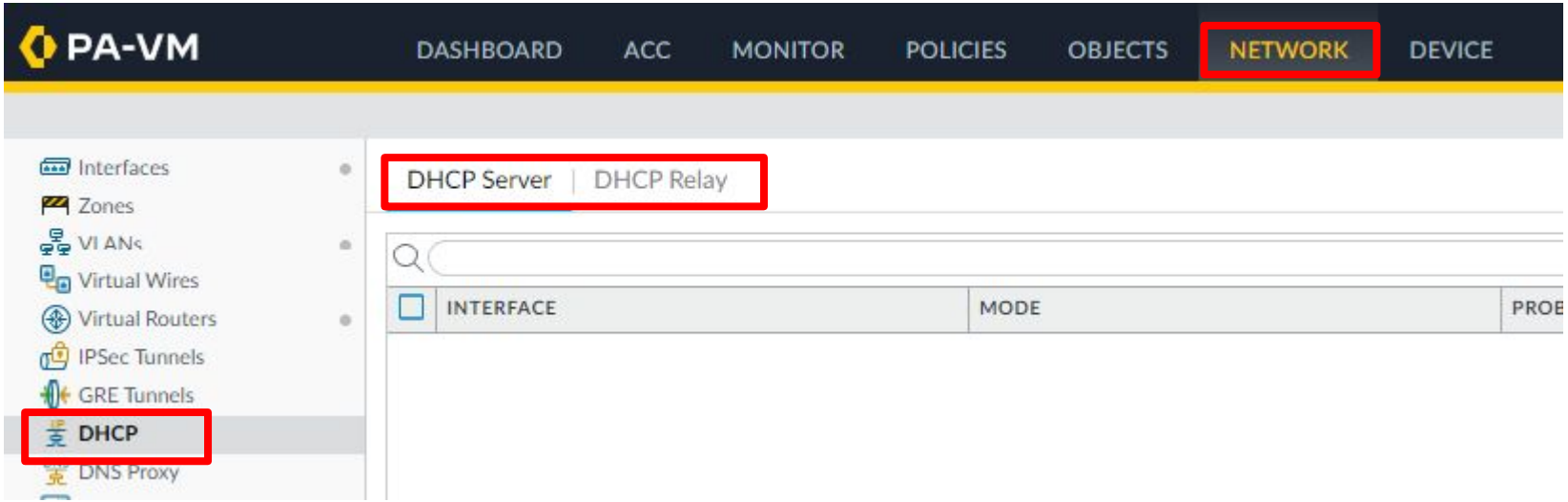


DHCP

DHCP

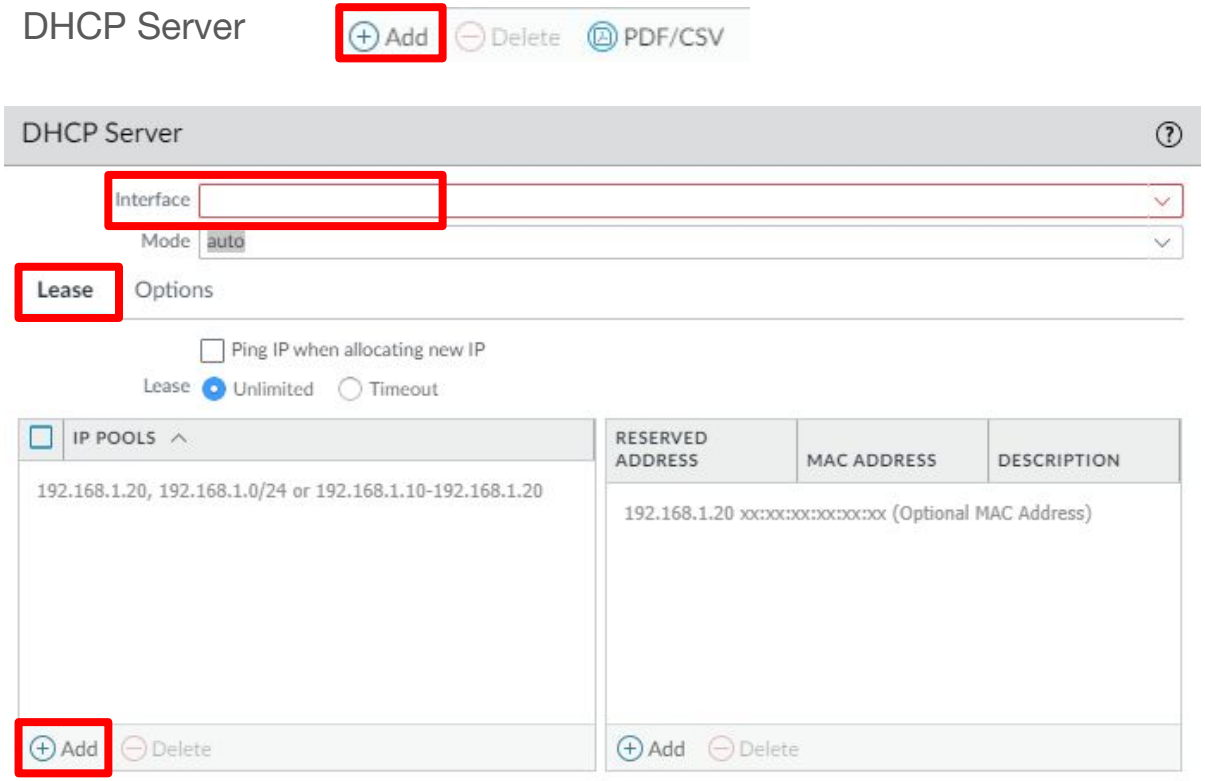
DHCP Server - Firewall is the source for IP Addressing

DHCP Relay - Firewall relays request to a server on a different subnet



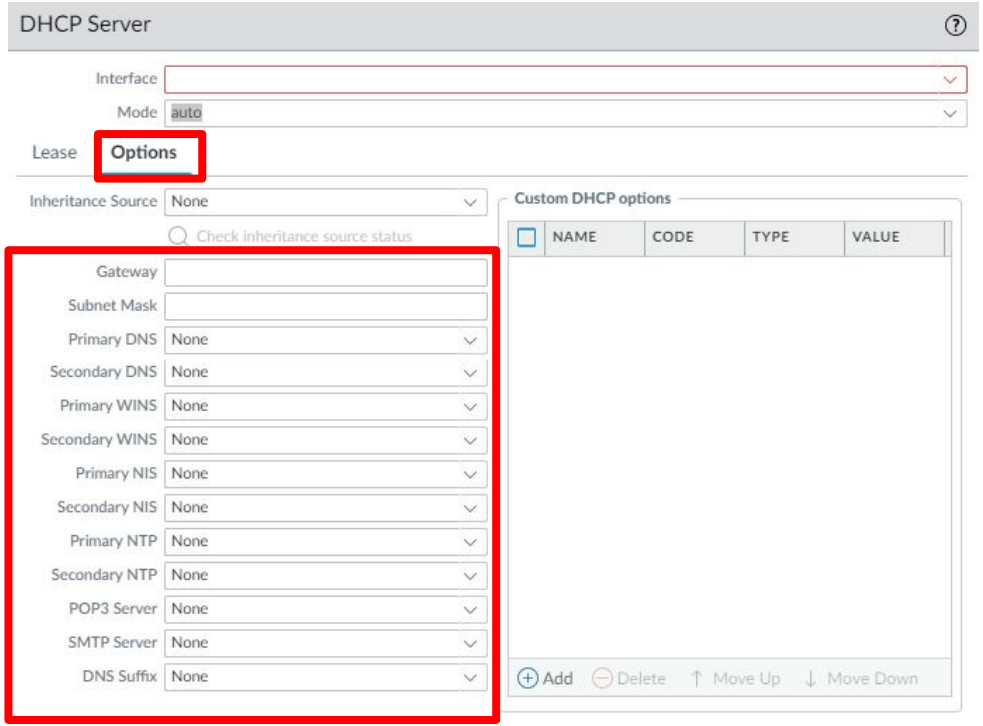
DHCP

DHCP Server



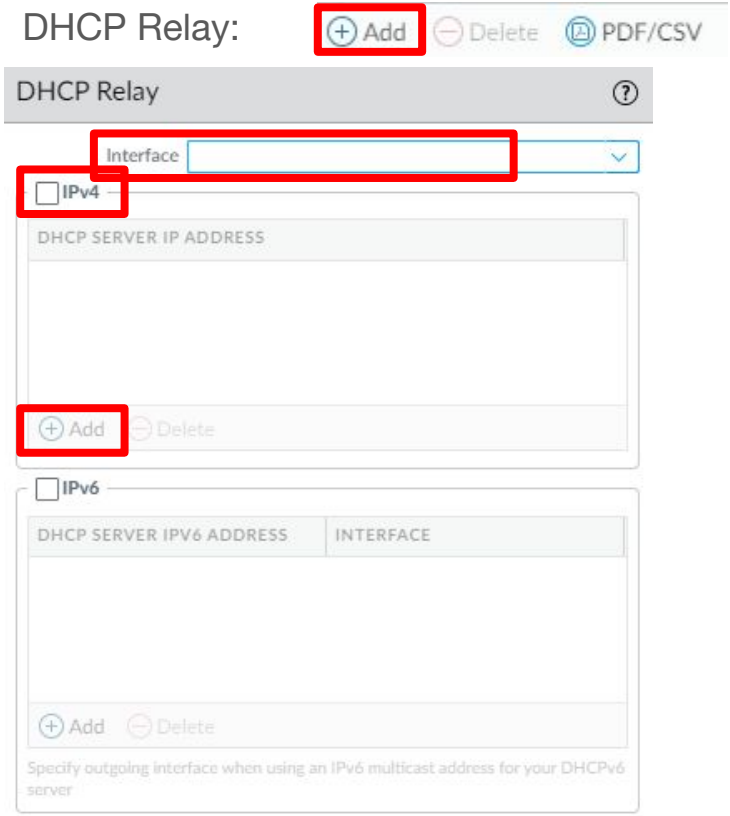
DHCP

DHCP Server: Options



DHCP

DHCP Relay:



NAT

NAT

Types of Network Address Translation (NAT) Policies:

Source NAT:

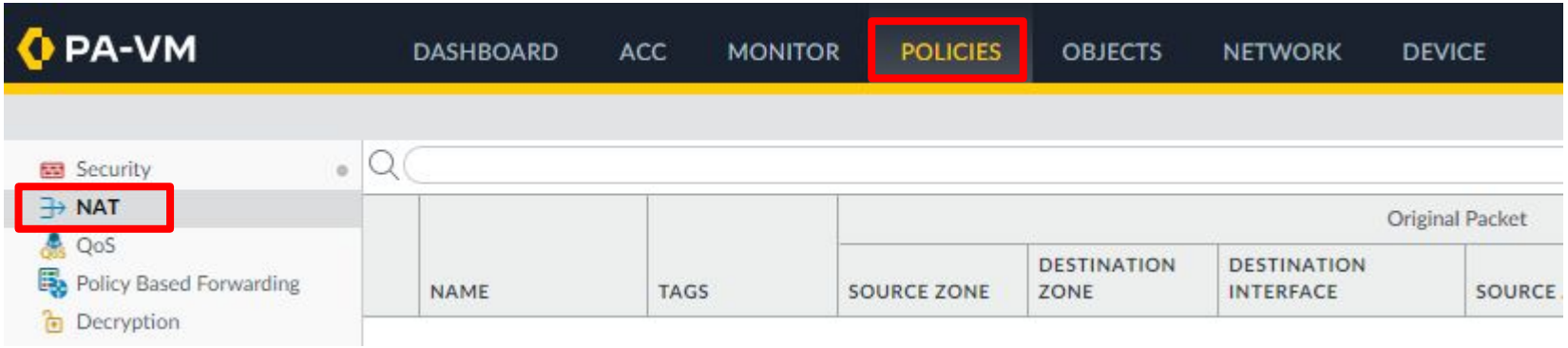
- Static IP - 1-to-1 translation to a defined address
- Dynamic IP - 1-to-1 translation to an address from a pool. Pool should match needs.
- Dynamic IP and Port (DIPP) - 1-to-1 translation to an address from a pool or interface. Pool does not match needs and multiple devices share the same IP and require a different port. Also called Port Address Translation (PAT)

Destination NAT:

- Static IP - 1-to-1 translation to a defined address
- Dynamic IP (with Session Disruption) - 1-to-1 translation to a dynamic IP on the destination device via FQDN.

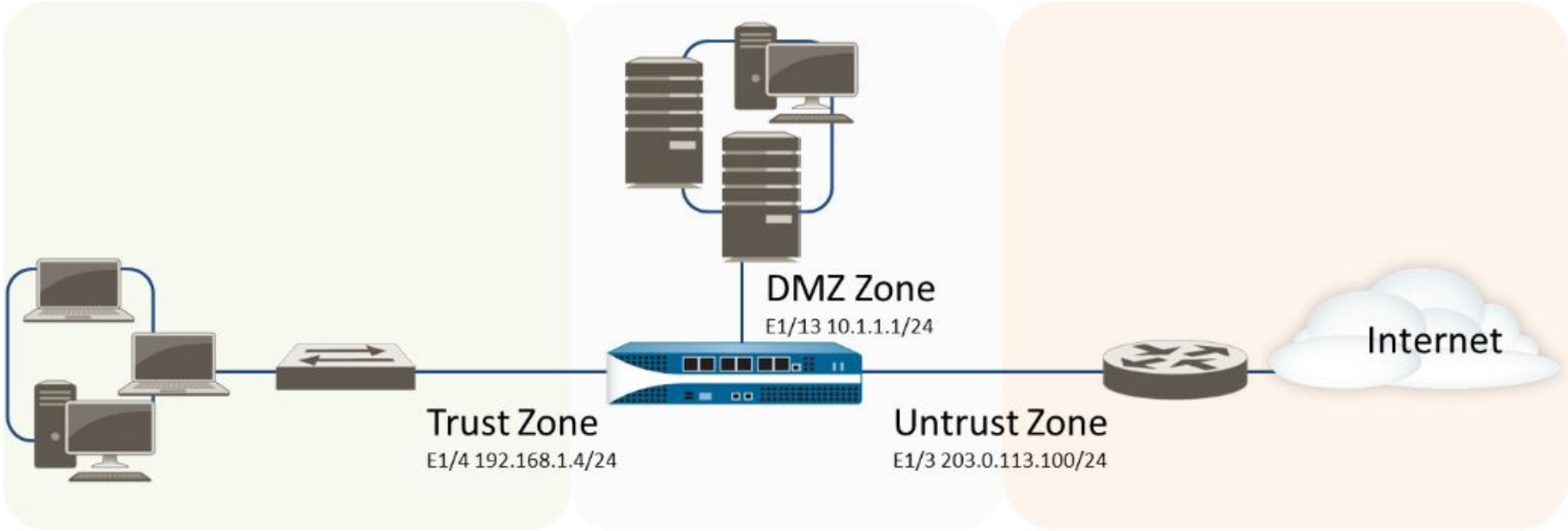
NAT

NAT Policies:



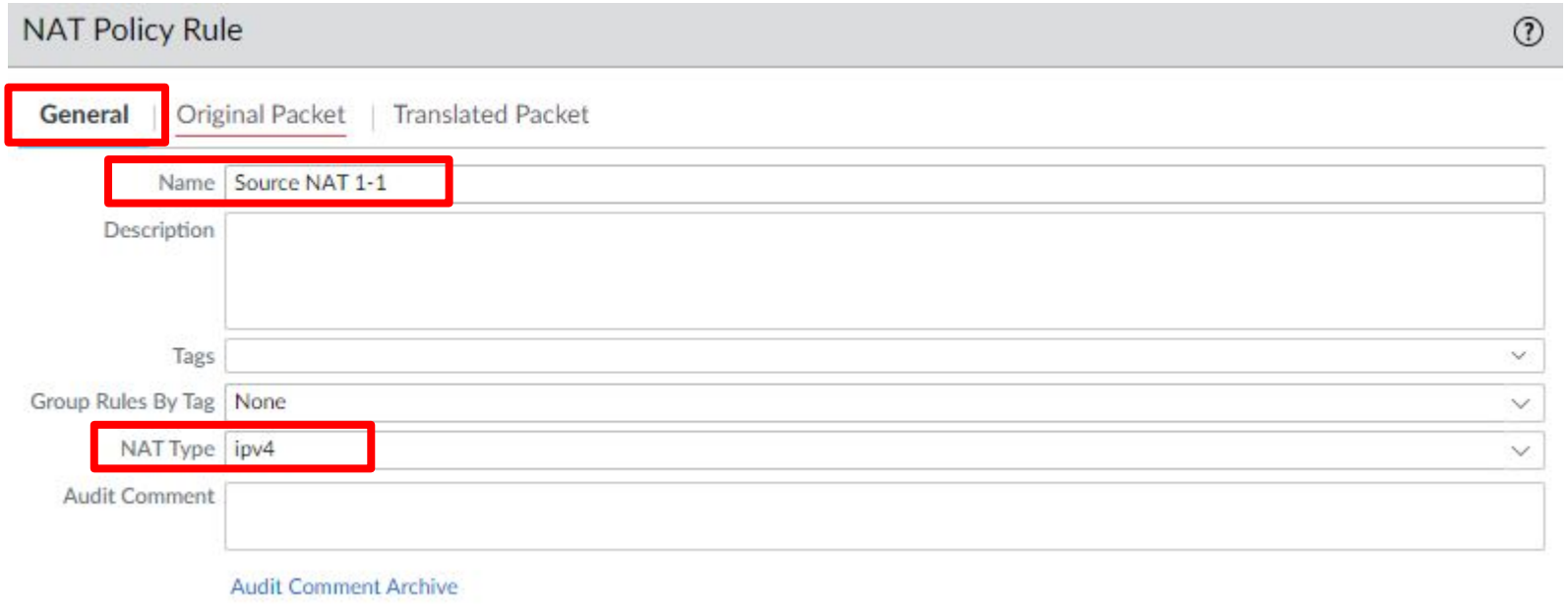
NAT

Source NAT:



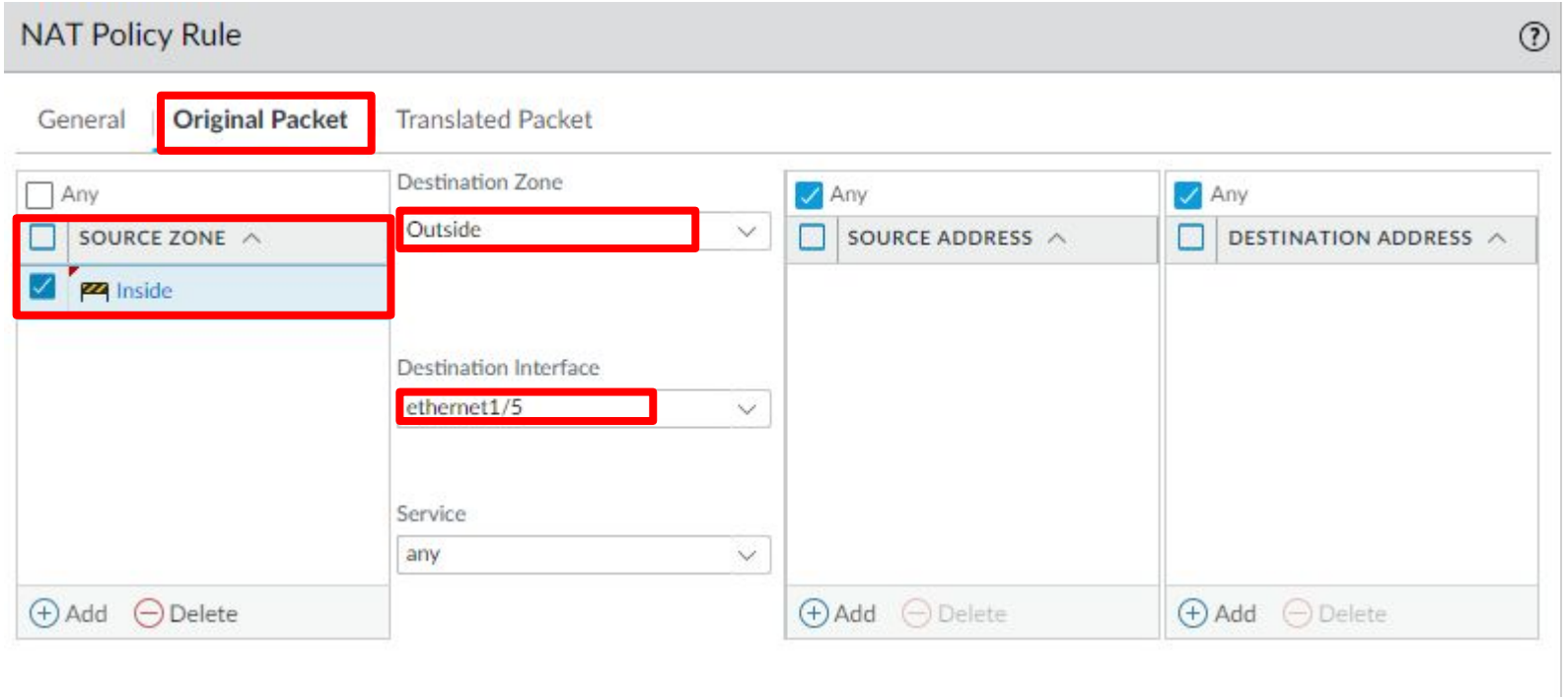
NAT

Source NAT Example:



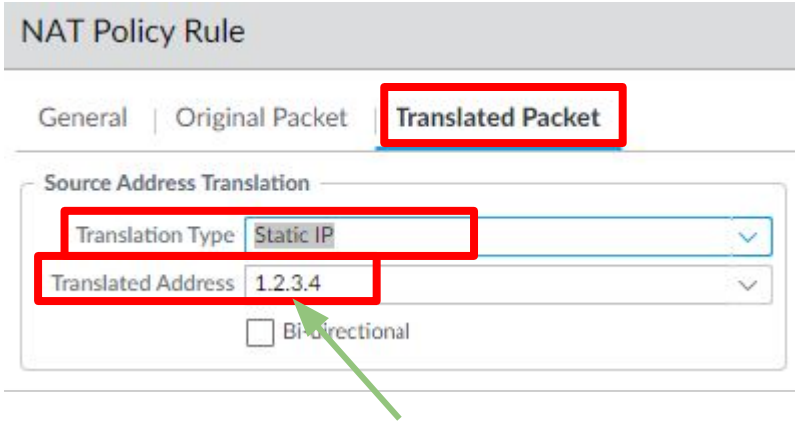
NAT

Source NAT Example:

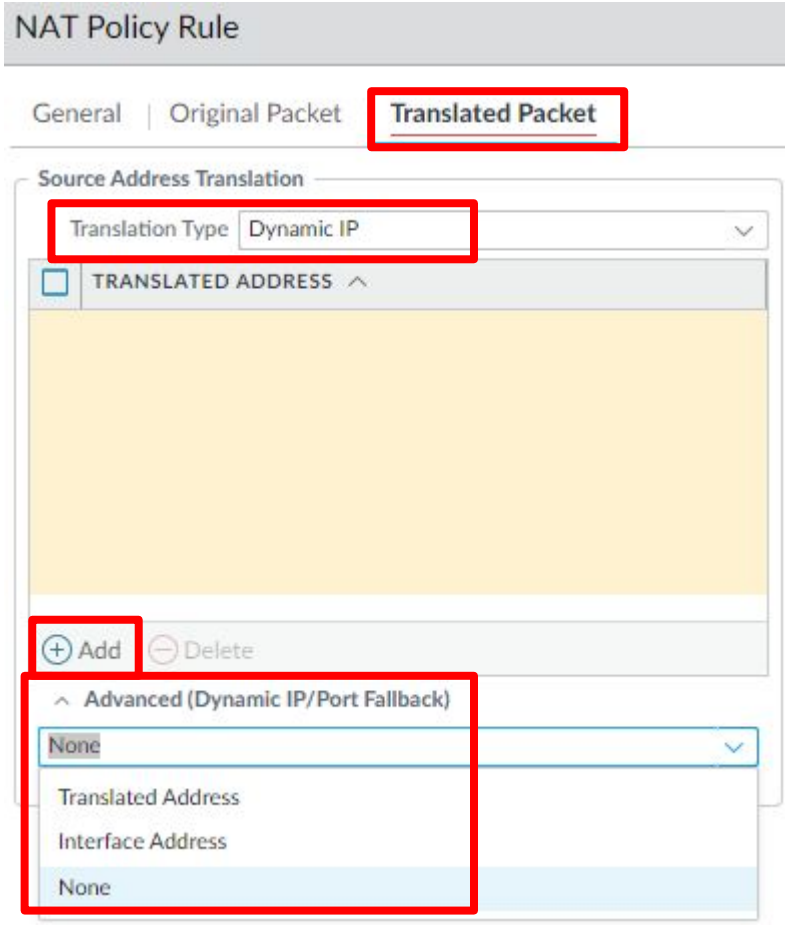


NAT

Source NAT Example:

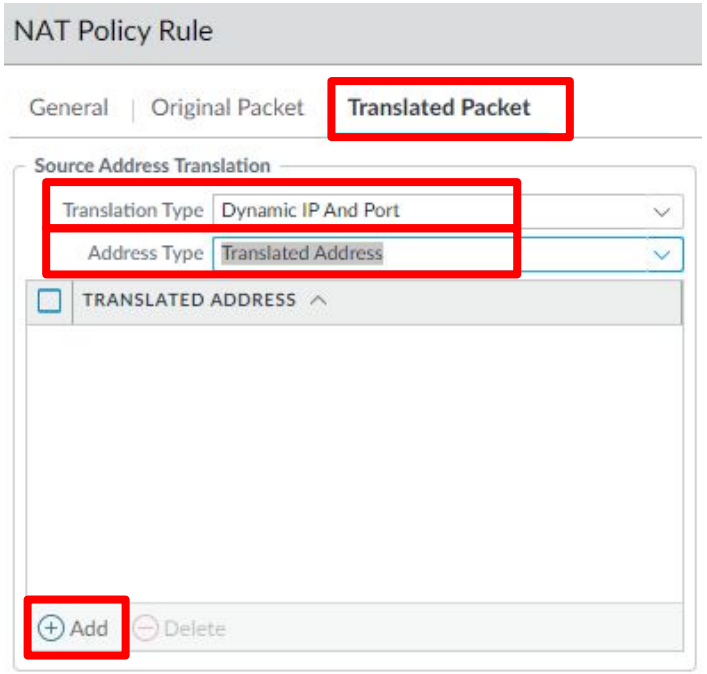


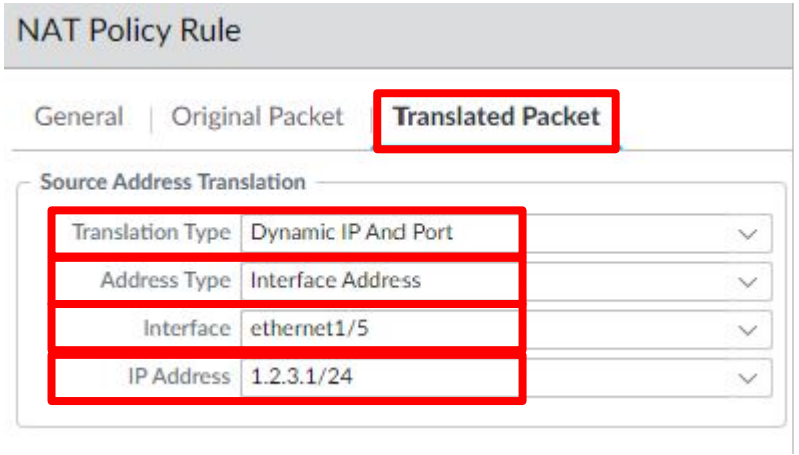
Static translation can be to a single address or a subnet of addresses. The subnet will translate to a 1-1 relationship. (i.e. 10.0.0.50 -> 100.0.0.50)



NAT

Source NAT Example:





NAT

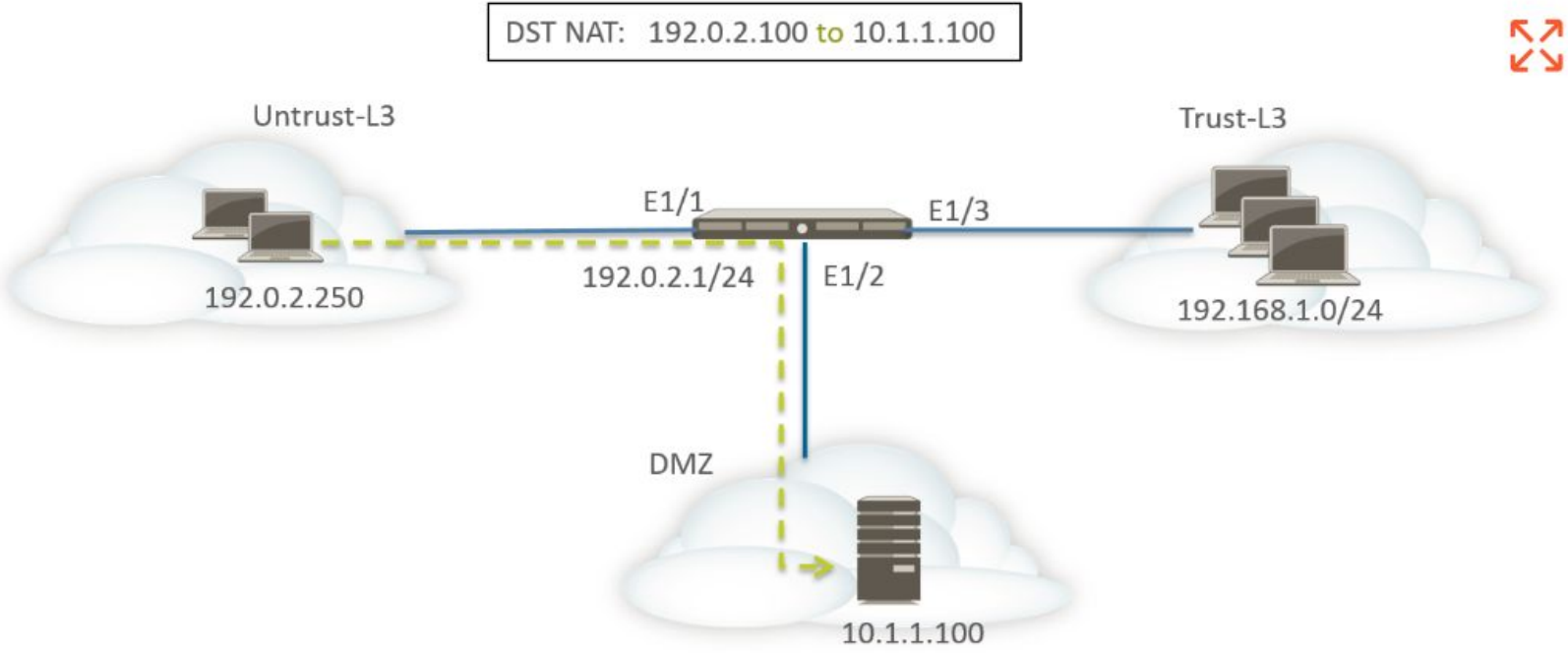
Multiple ISP NAT:

- If you have multiple ISPs, you need multiple NAT policies.

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	ISP-1-NAT-Hub	none	inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 10.4.0.2/30	none
2	ISP-2-NAT-Hub	none	inside	outside	ethernet1/2	any	any	any	dynamic-ip-and-port ethernet1/2 10.4.1.2/30	none

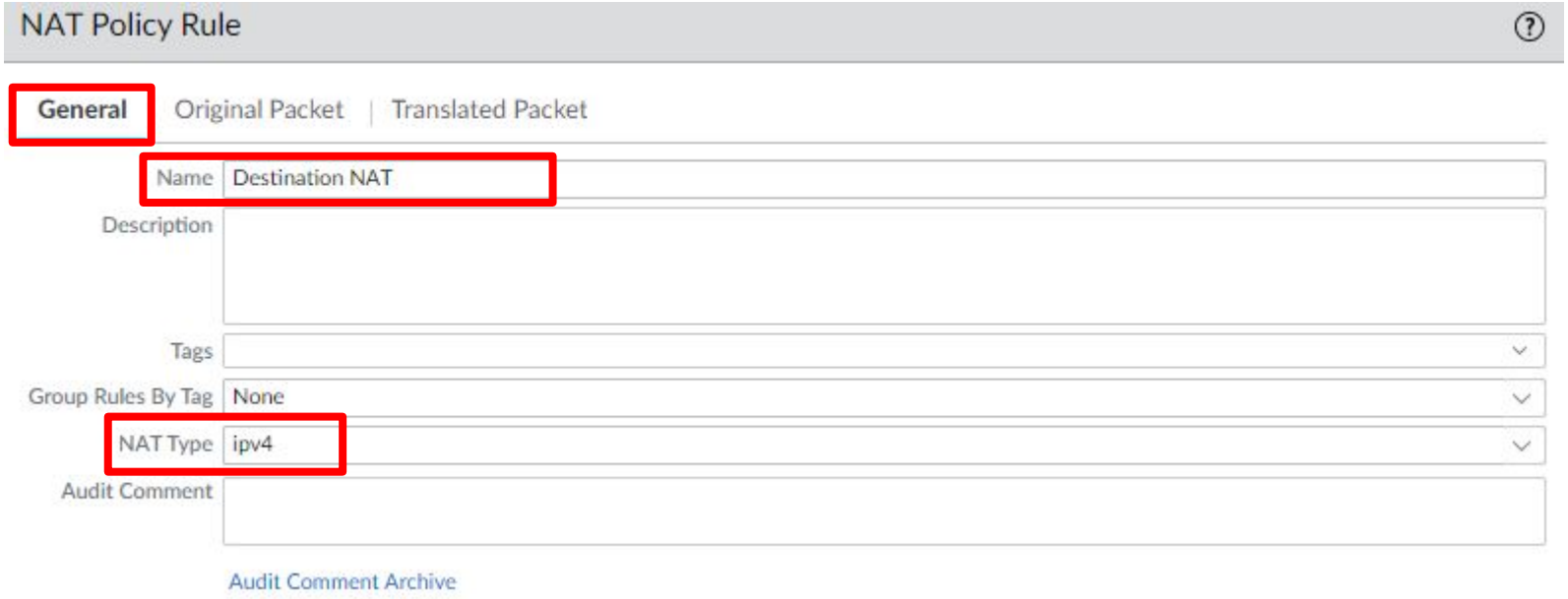
NAT

Destination NAT:



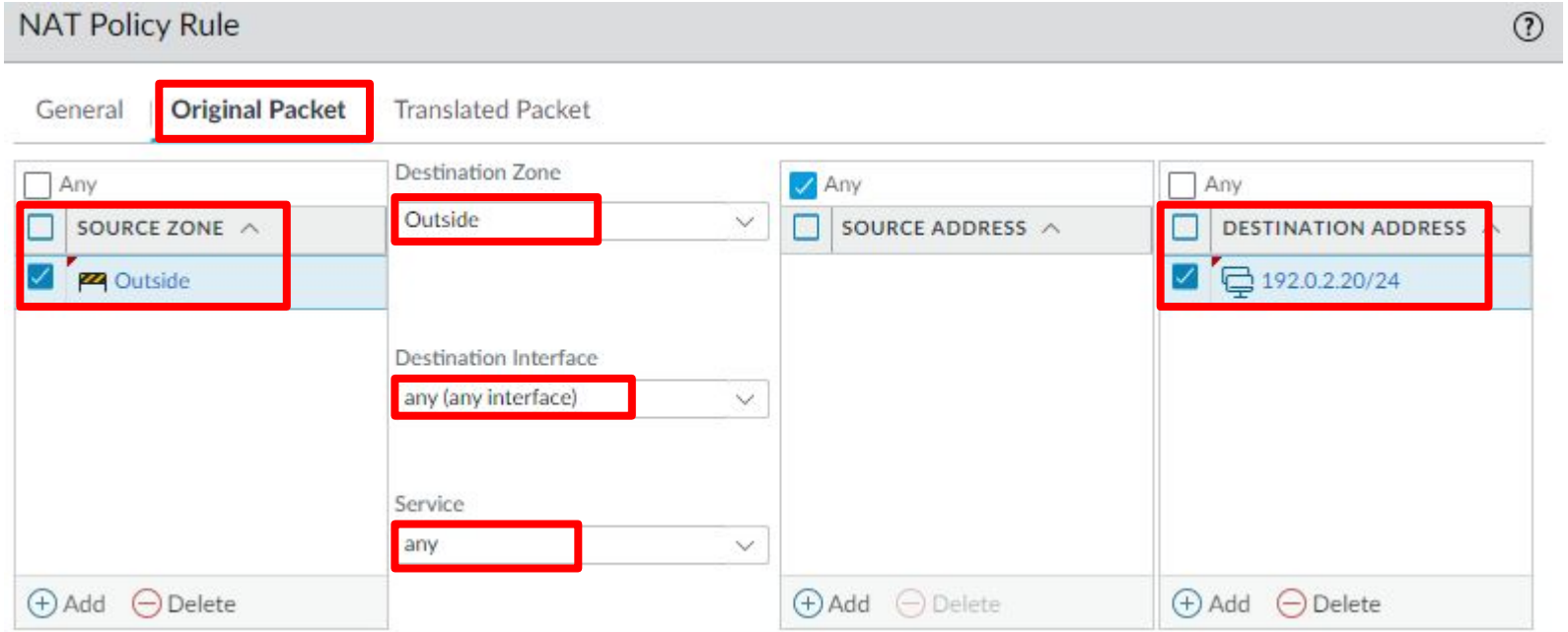
NAT

Destination NAT Example:



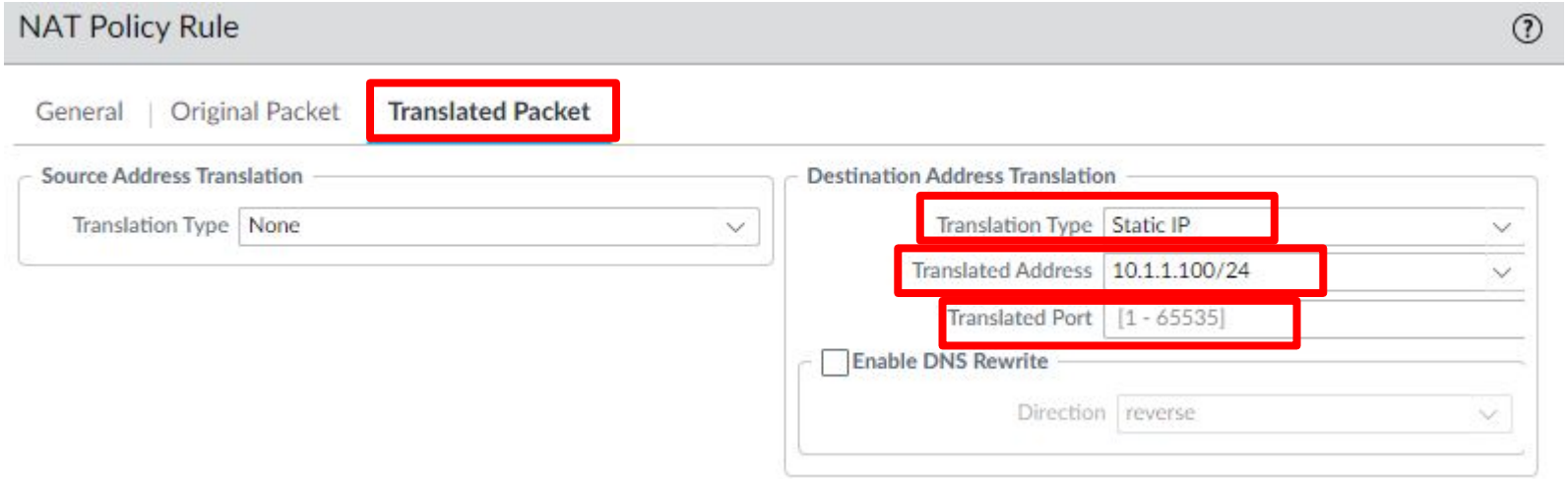
NAT

Destination NAT Example:



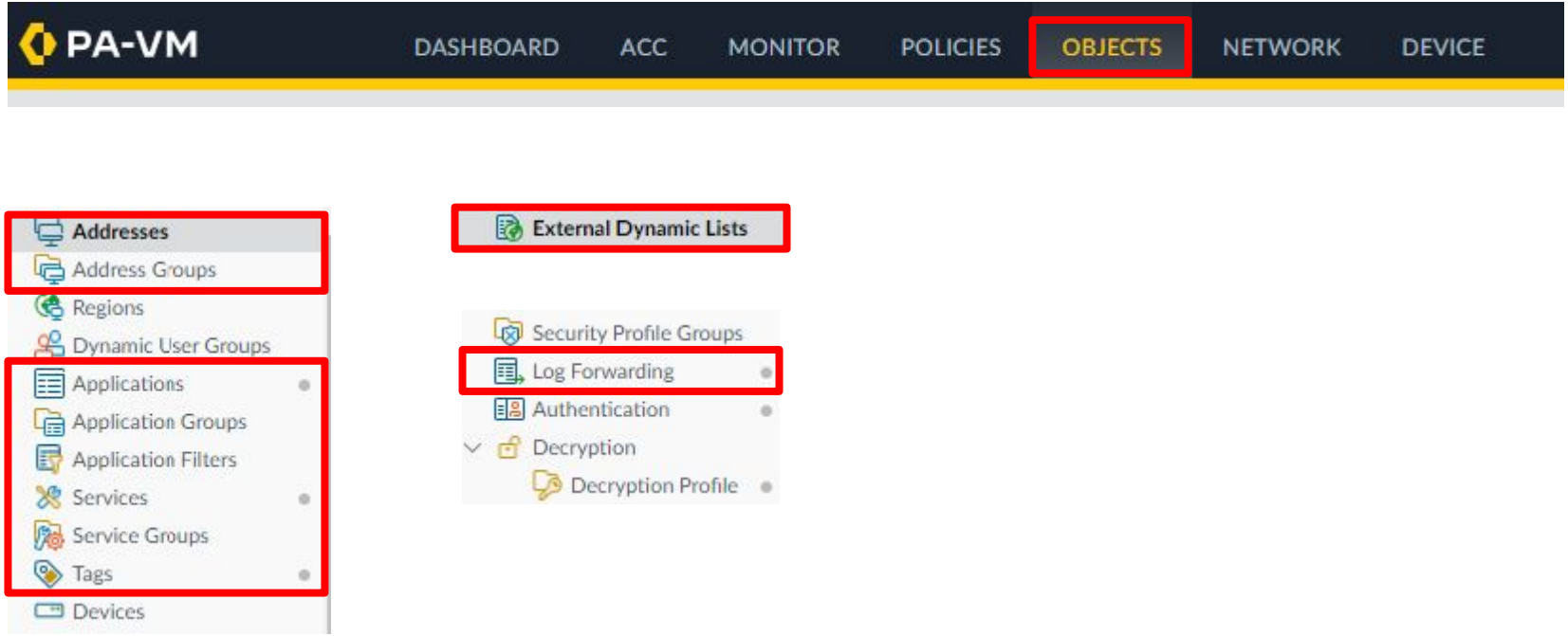
NAT

Destination NAT Example:



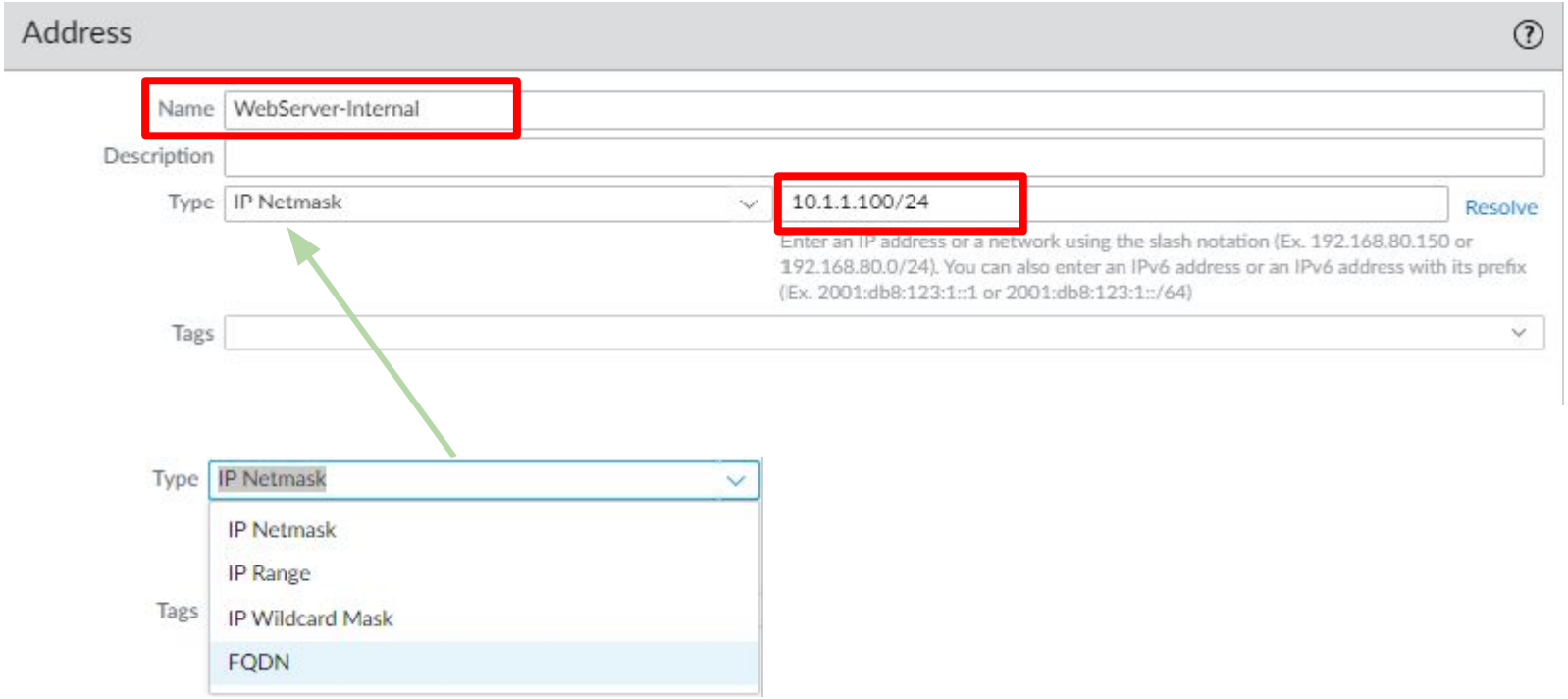
Objects

Objects



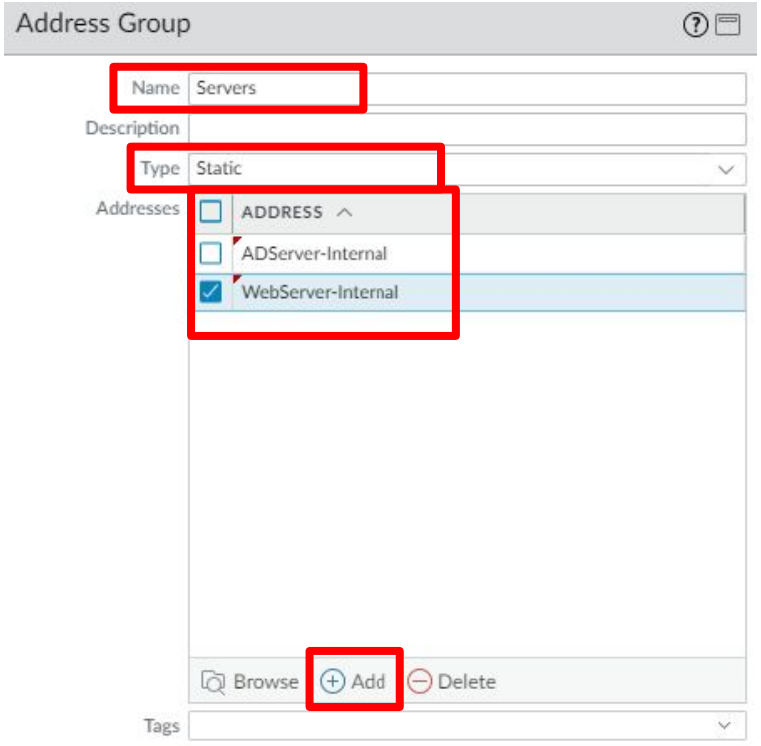
Objects

Addresses:



Objects

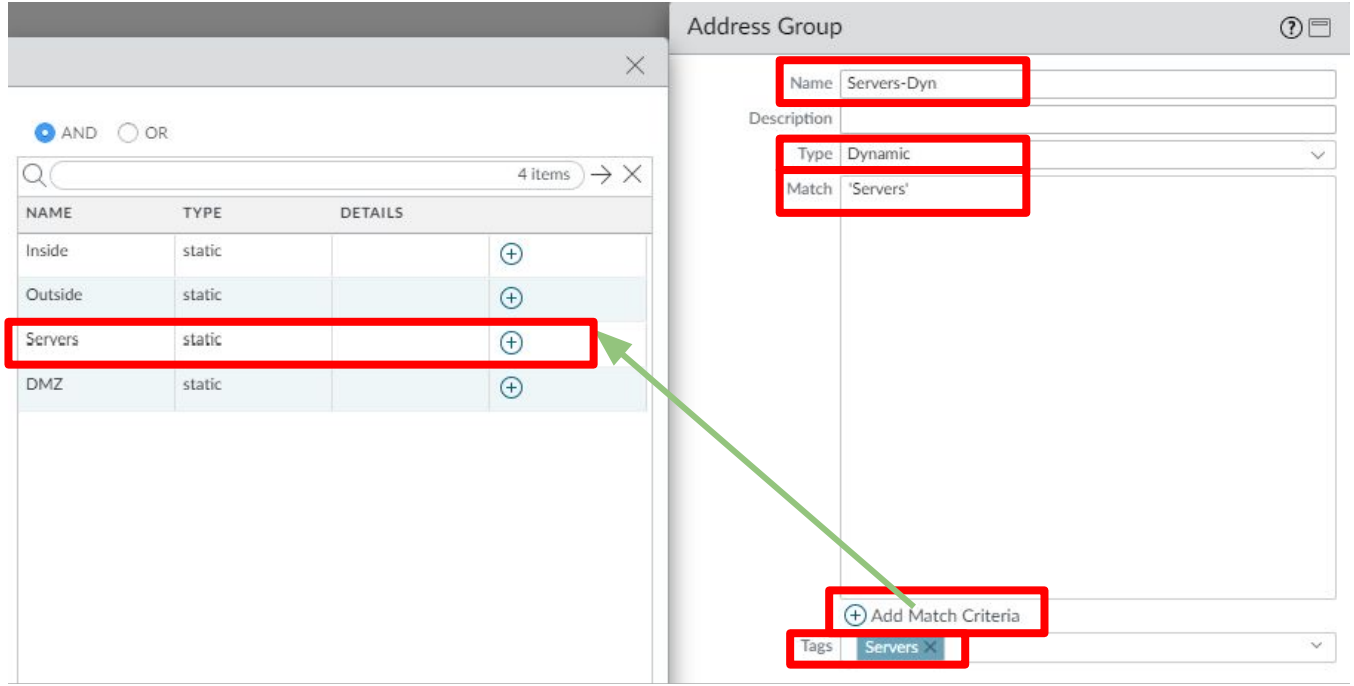
Address Groups: Static



Objects

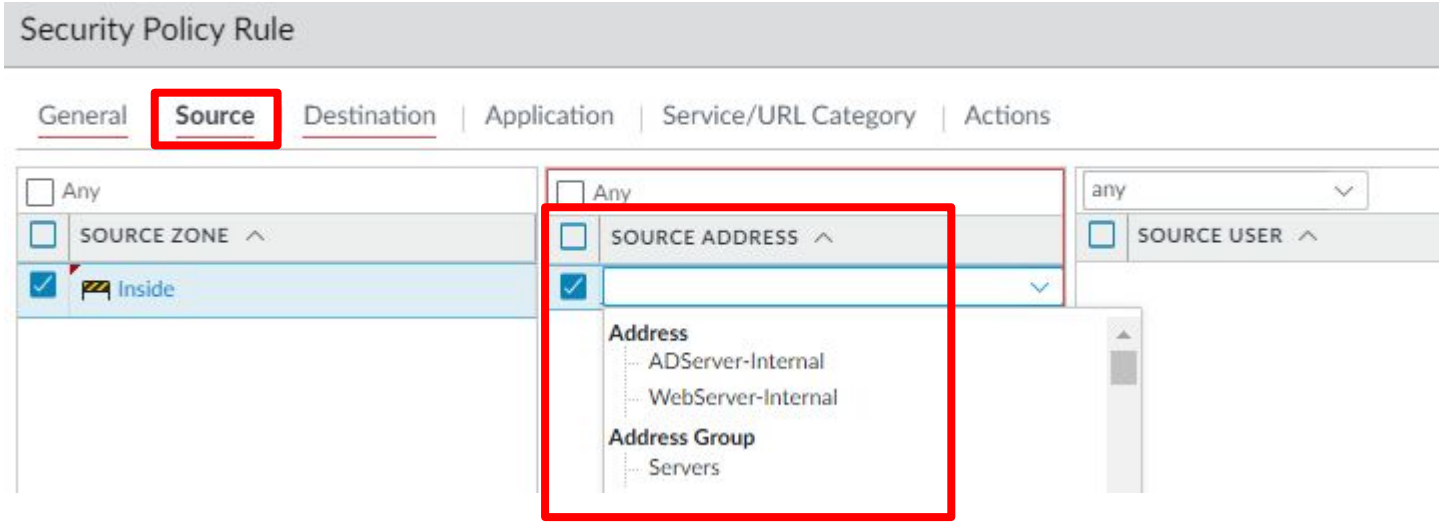
Address Groups: Dynamic

DAG needs to be used in a Policy to populate.



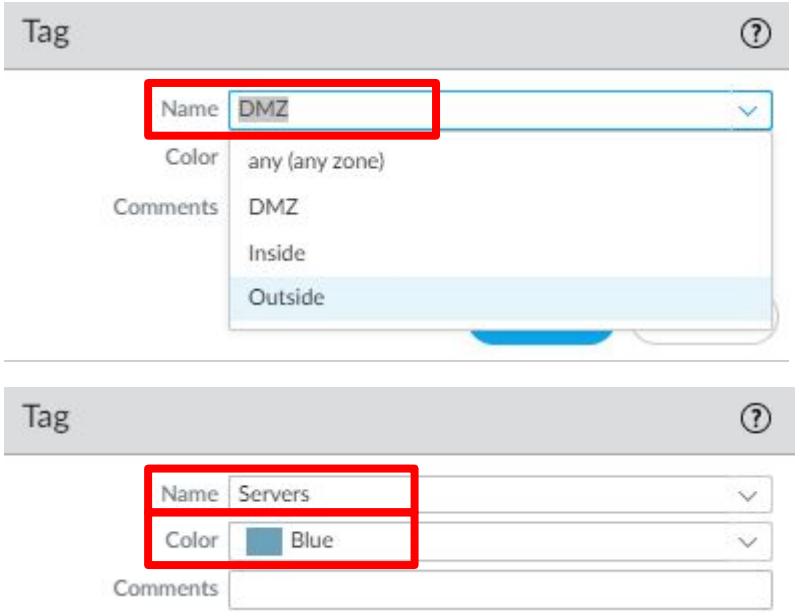
Objects

Addresses and Address Groups Use:



Objects

Tags:

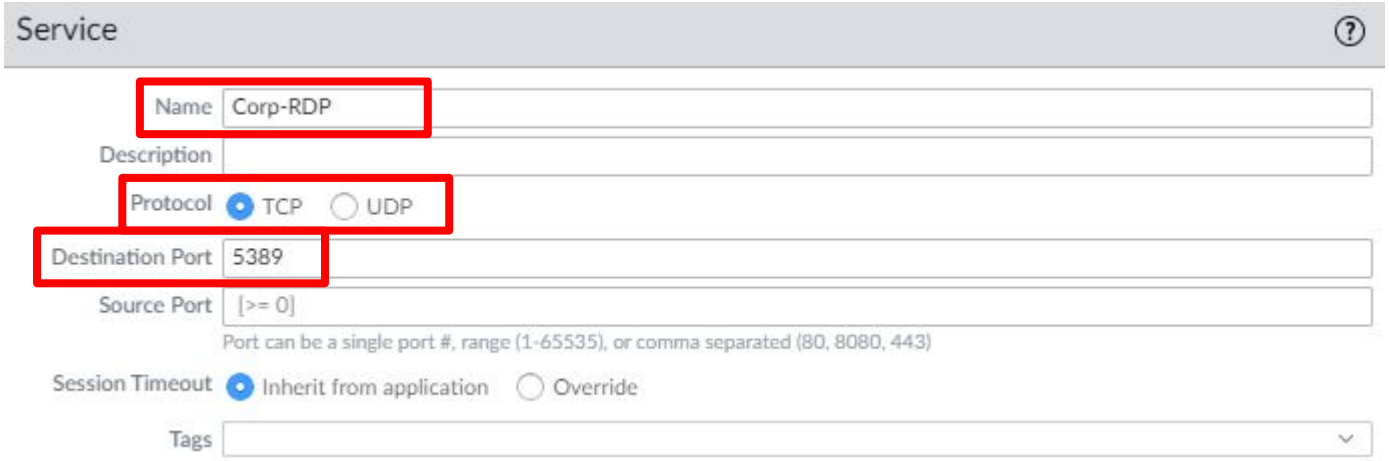


Zones Automatically populate to create tags

Ability to create custom tags

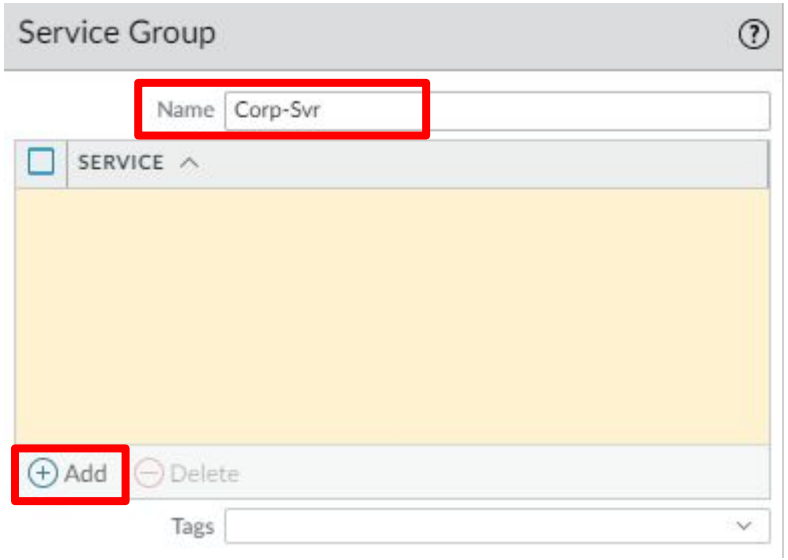
Objects

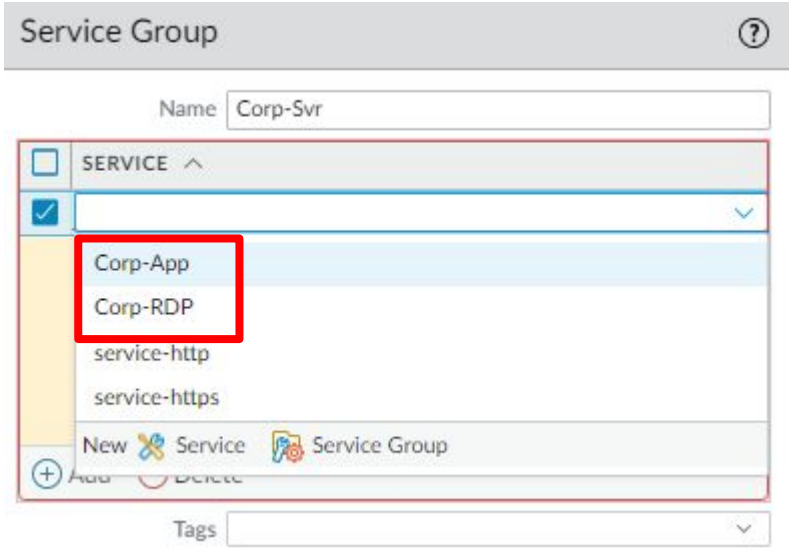
Services:



Objects

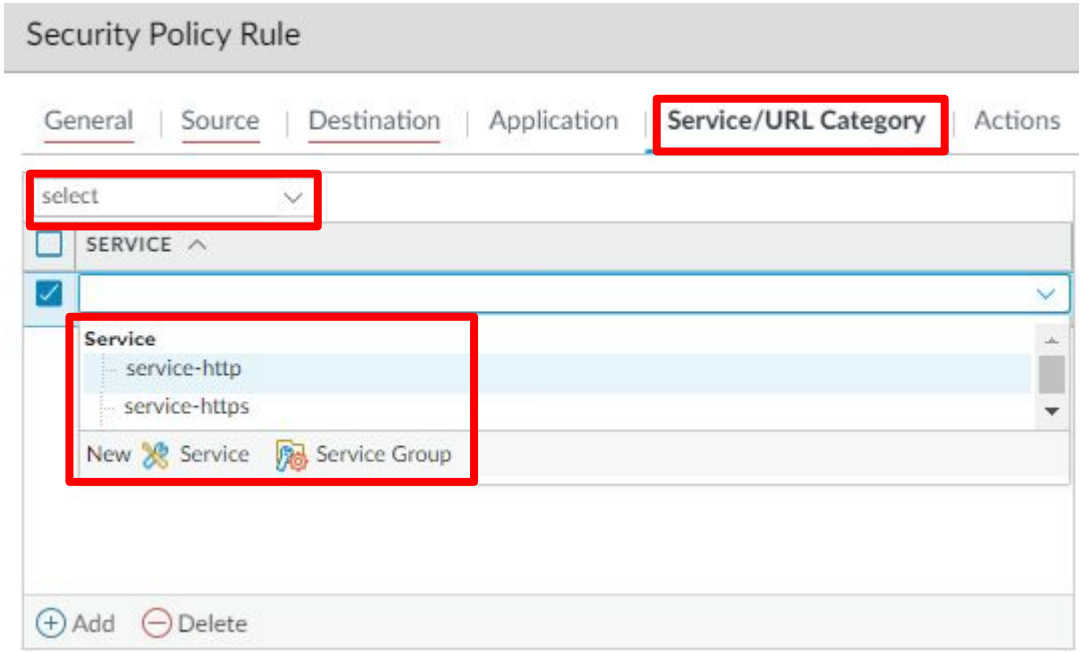
Service Groups:





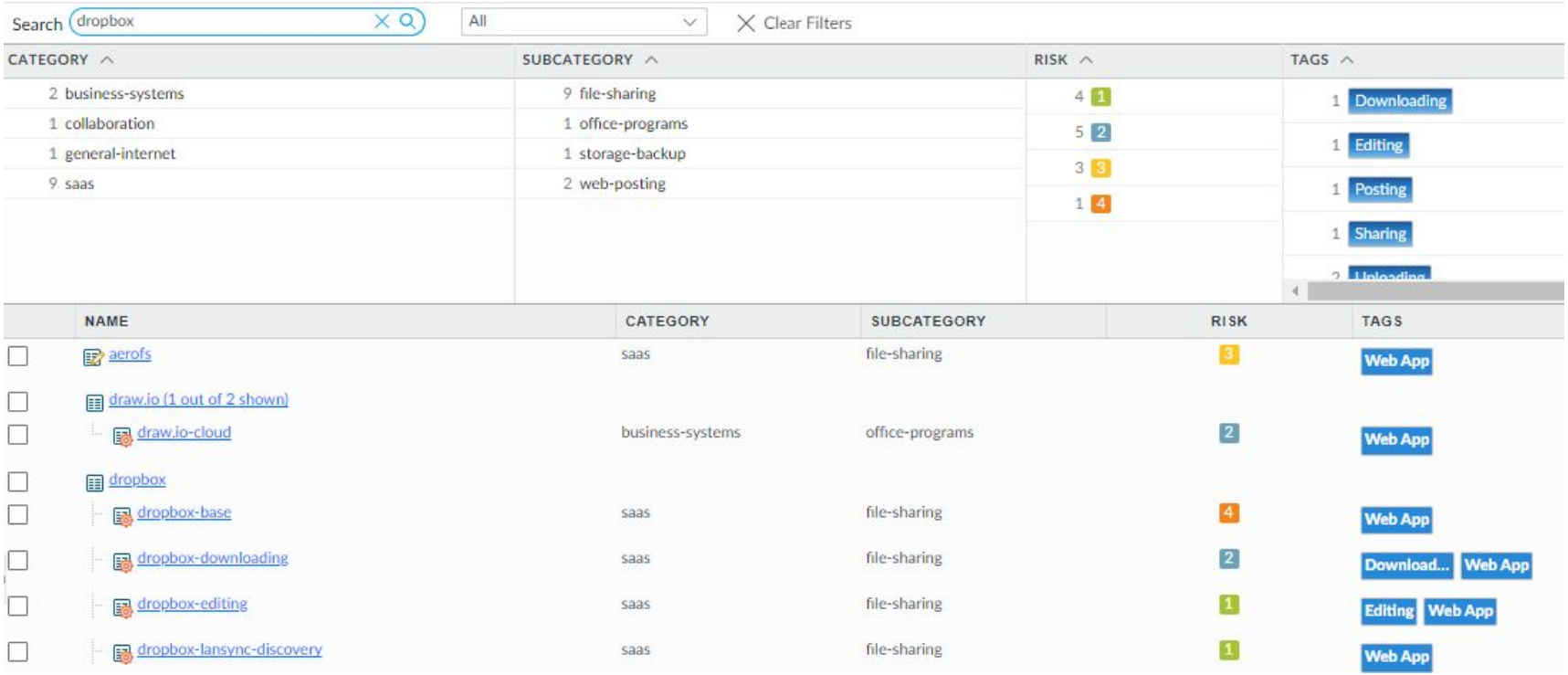
Objects

Service and Service Group Usage:



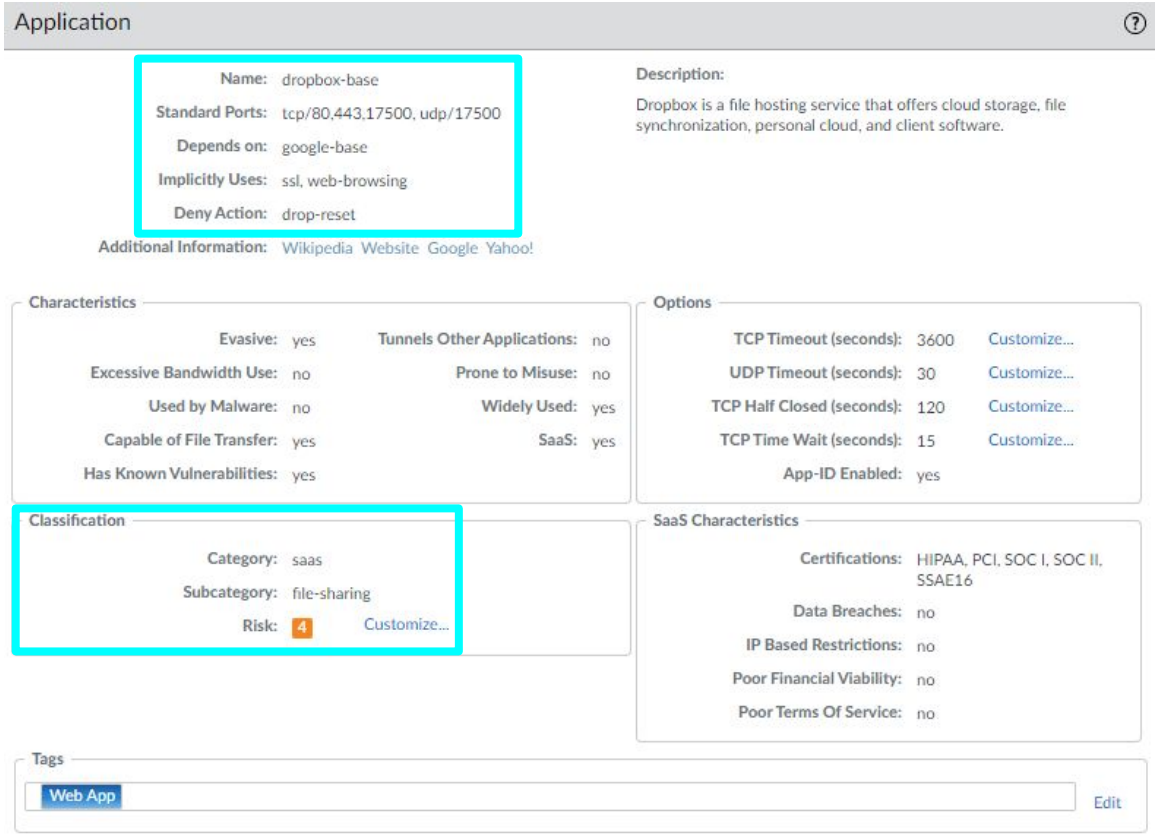
Objects

Applications:



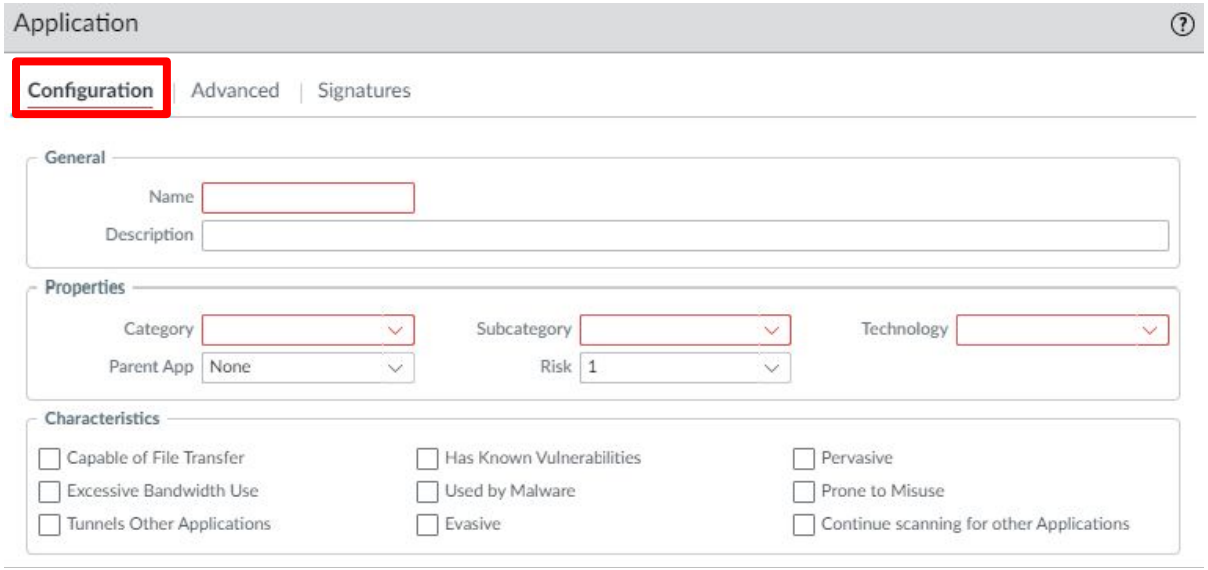
Objects

Applications:



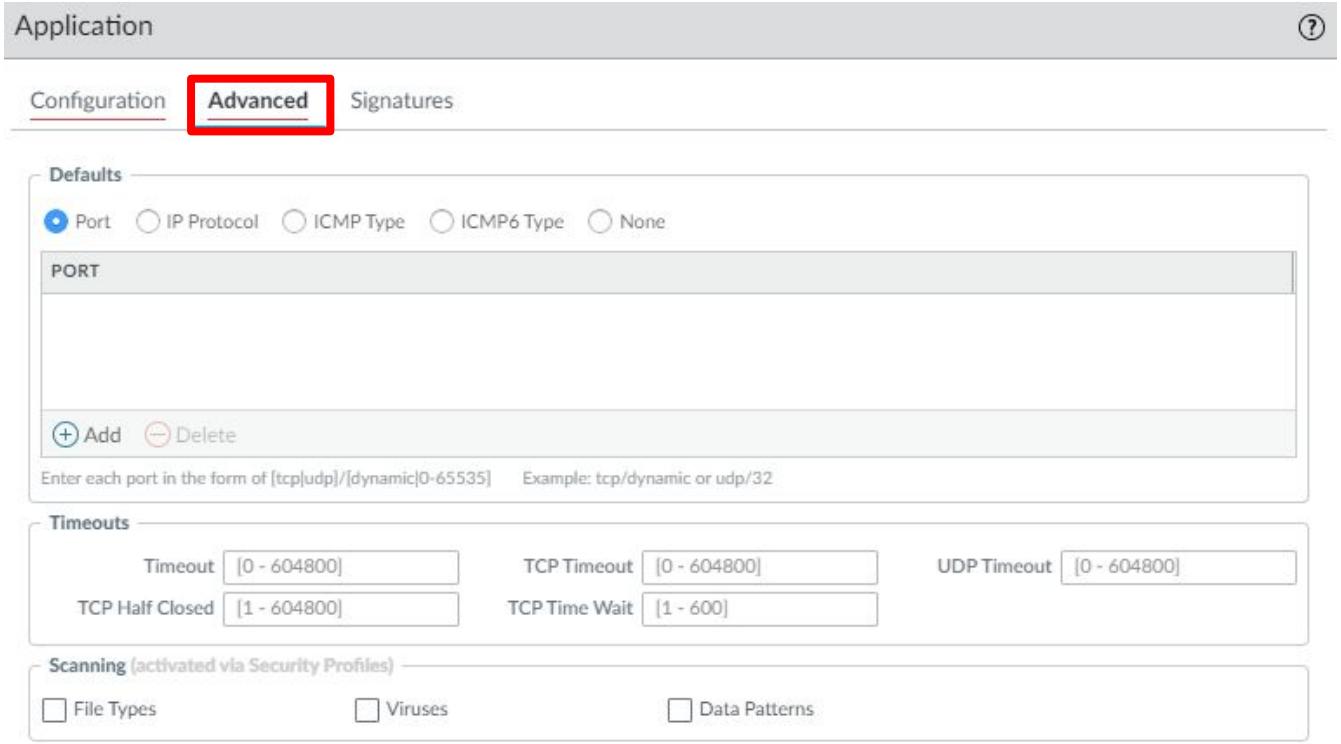
Objects

Applications: Custom



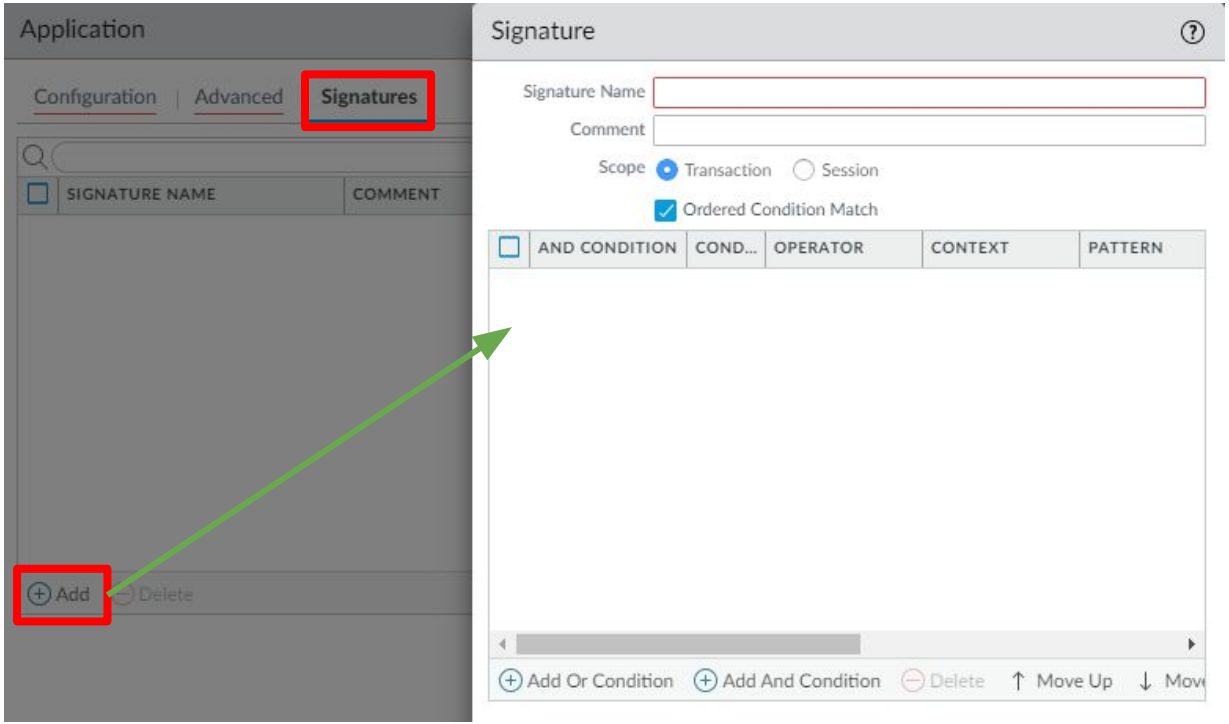
Objects

Application: Custom



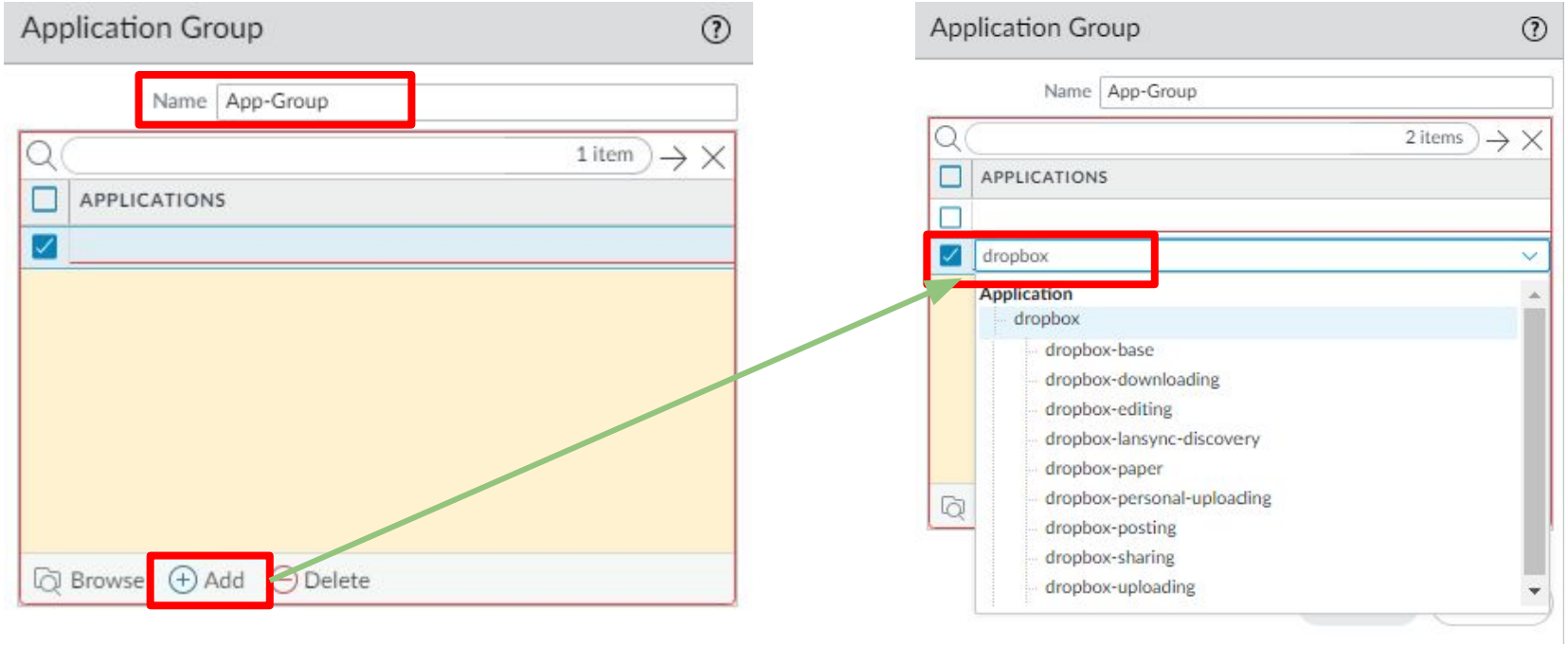
Objects

Application: Custom



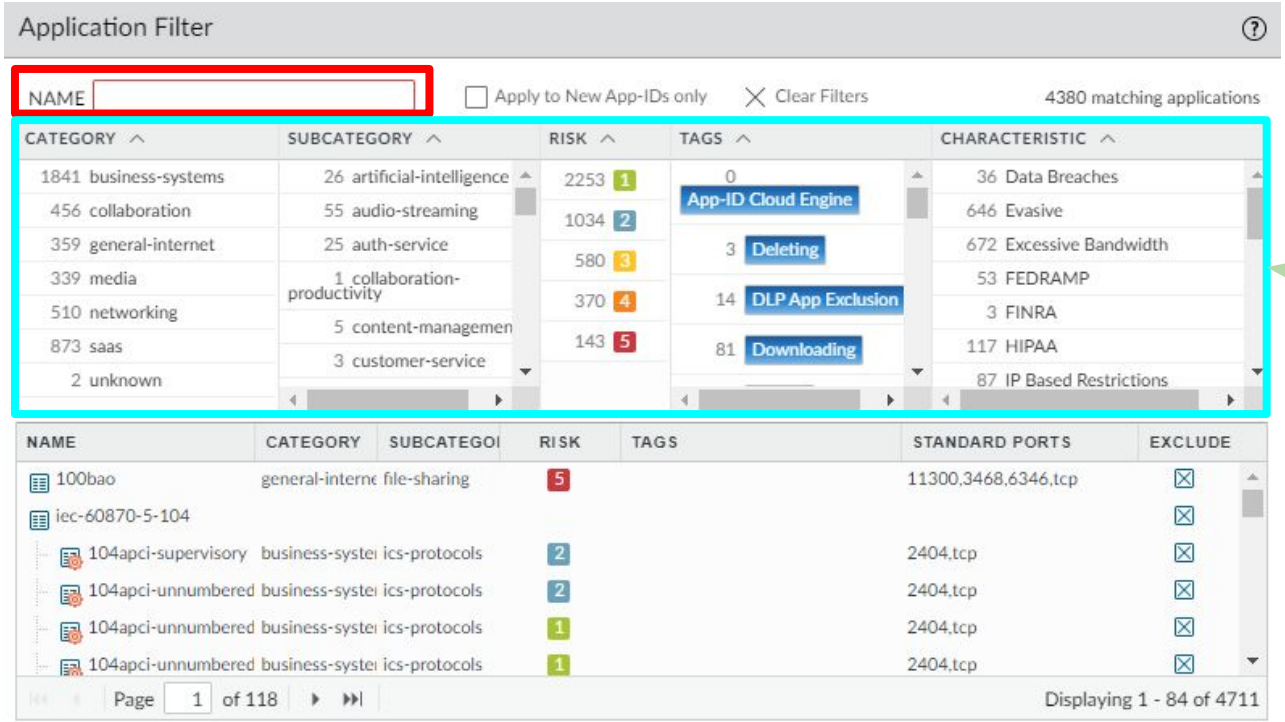
Objects

Application Groups: Static



Objects:

Application Filters: Dynamic



Select what will be used to filter for applications (Category, Subcategory, Risk Level, Tag, Characteristic)

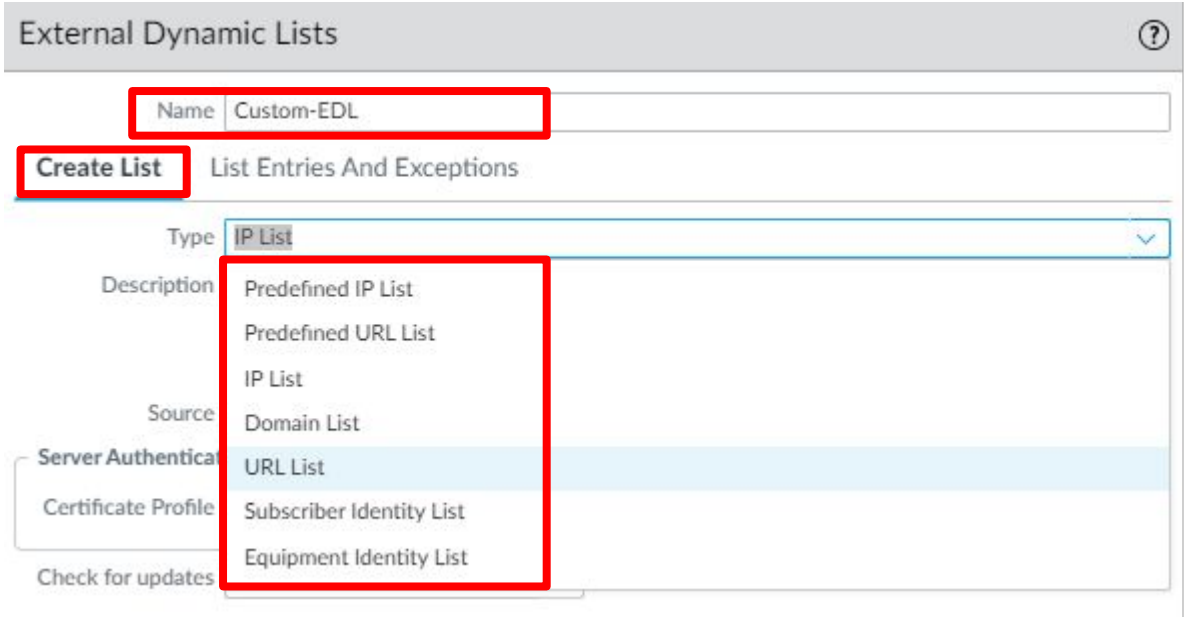
Objects:

External Dynamic Lists: Predefined

NAME	LOCATION	DESCRIPTION	SOURCE
Dynamic IP Lists			
Palo Alto Networks - Tor exit IP addresses	Predefined	IP addresses supplied by multiple providers and validated with Palo Alto Networks threat intelligence data as active Tor exit nodes. Traffic from Tor exit nodes can serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments.	panw-torexit-ip-list
Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	panw-bulletproof-ip-list
Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	panw-highrisk-ip-list
Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	panw-known-ip-list
Dynamic URL Lists			
Palo Alto Networks - Authentication Portal Exclude List	Predefined	Domains and URLs to exclude from Authentication Policy. This list is managed by Palo Alto Networks.	Palo Alto Networks - Authentication Portal Exclude List

Objects:

External Dynamic List: Custom



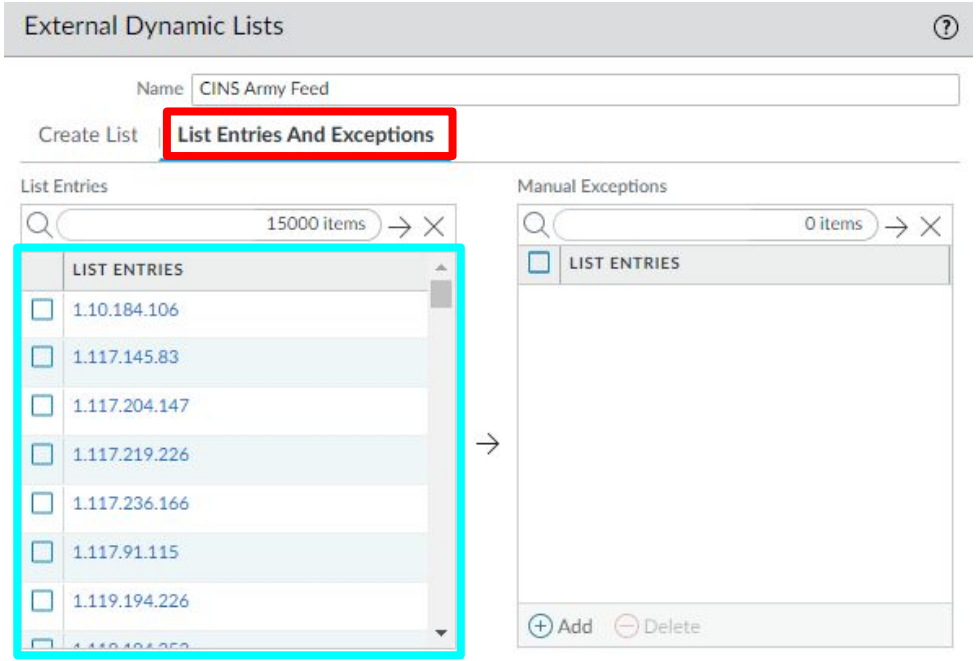
Objects:

External Dynamic List: Custom

Objects

Custom EDL:

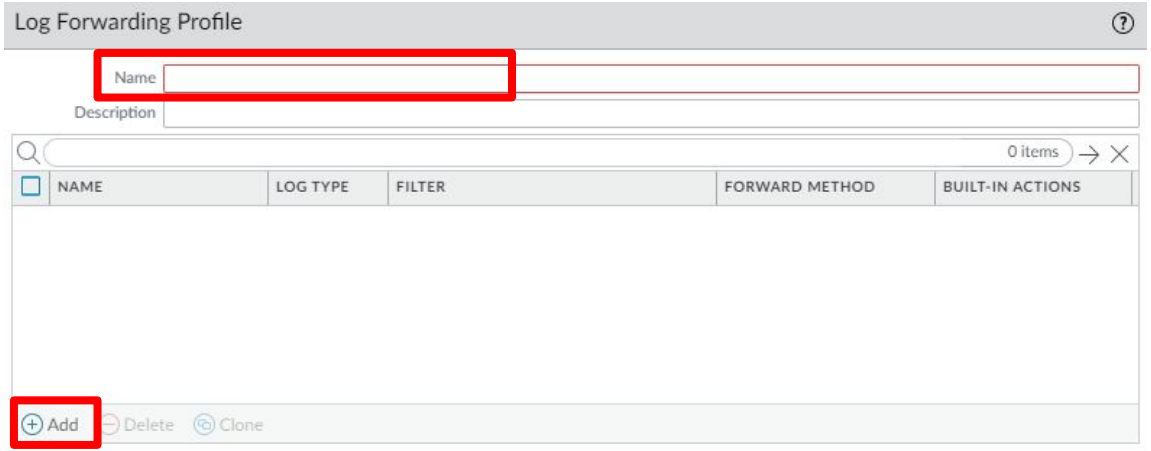
Lists must be applied to a policy to retrieve information from server.



Objects:

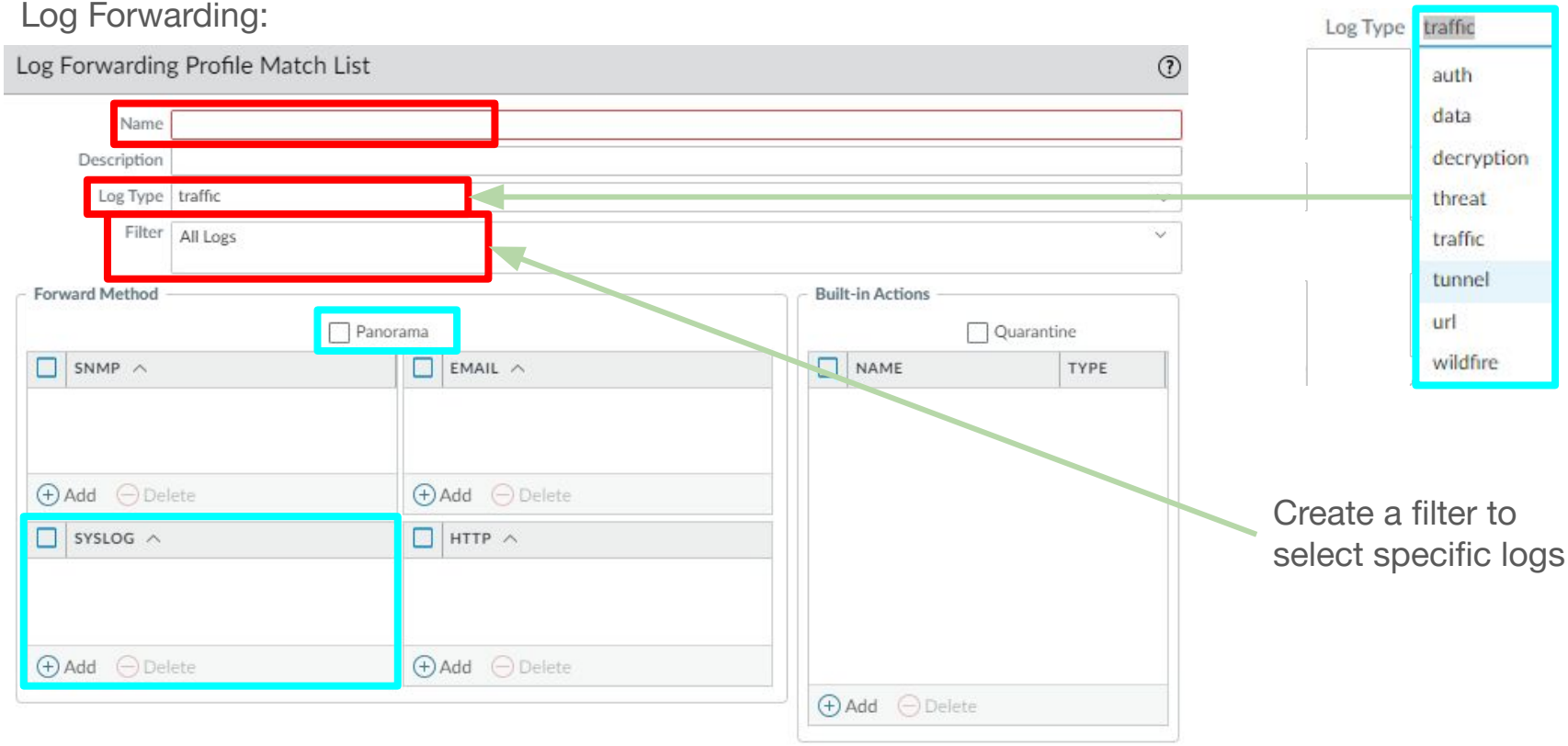
Log Forwarding:

NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP
IoT Security Default Profile	Predefined		traffic	All Logs	☑				
			threat	All Logs	☑				
			wildfire	All Logs	☑				
			url	All Logs	☑				
			data	All Logs	☑				
			tunnel	All Logs	☑				
			auth	All Logs	☑				
			decryption	All Logs	☑				



Objects:

Log Forwarding:



Licenses and Profiles

Licenses

Subscription Licenses and CDSS

- Advanced Threat Prevention
- Advanced URL Filtering
- Advanced Wildfire
- DNS Security - Requires ATP
- SD-WAN - Requires Panorama

Part of the Core Security Bundle (CoreSec)

- GlobalProtect Gateway
- Internet of Things (IoT) Security
- Enterprise Data Loss Prevention (DLP)
- SaaS Security Inline
- Support
- Virtual Systems (vSys)
- Strata Cloud Manager Pro
- Strata Logging Service (Formally Cortex Data Lake or CDL)

Licenses

What happens when subscriptions expire: Docs Link

Palo Alto Networks subscriptions provide the firewall with added functionality and/or access to a Palo Alto Networks cloud-delivered service. When a license is within 30 days of expiration, a warning message displays in the system log daily until the subscription is renewed or expires. Upon license expiration, some subscriptions continue to function in a limited capacity, and others stop operating completely. Here you can find out what happens when each subscription expires.

The precise moment of license expiry is at the beginning of the following day at 12:00 AM (GMT). For example, if your license is scheduled to end on 1/20 you will have functionality for the remainder of that day. At the start of the new day on 1/21 at 12:00 AM (GMT), the license will expire. All license-related functions operate on Greenwich Mean Time (GMT), regardless of the configured time zone on the firewall.

DNS Security

You can still:

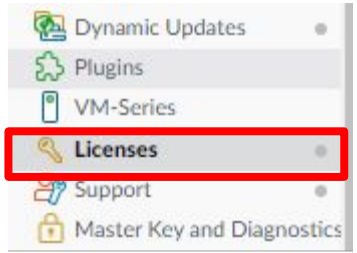
- Use local DNS signatures if you have an active Threat Prevention license.

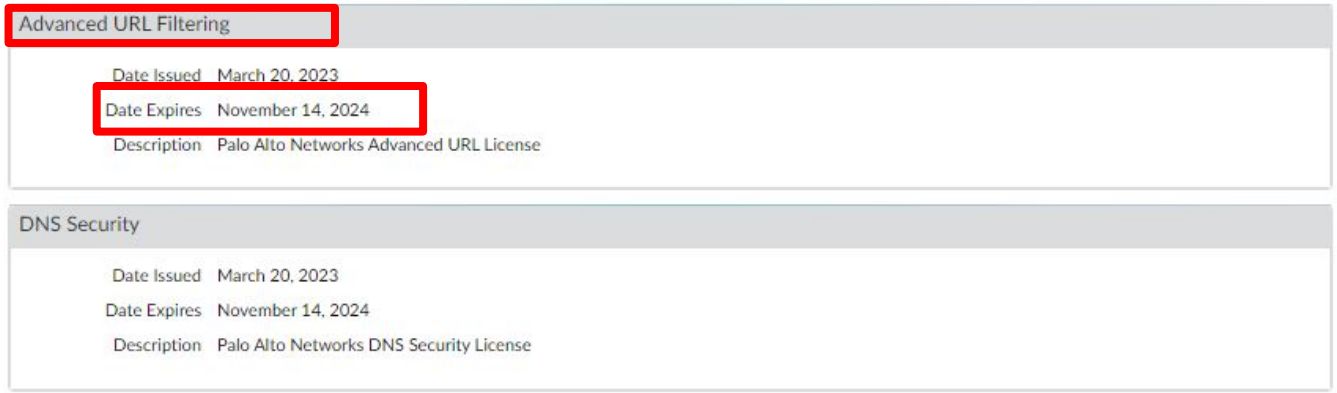
You can no longer:

- Get new DNS signatures.

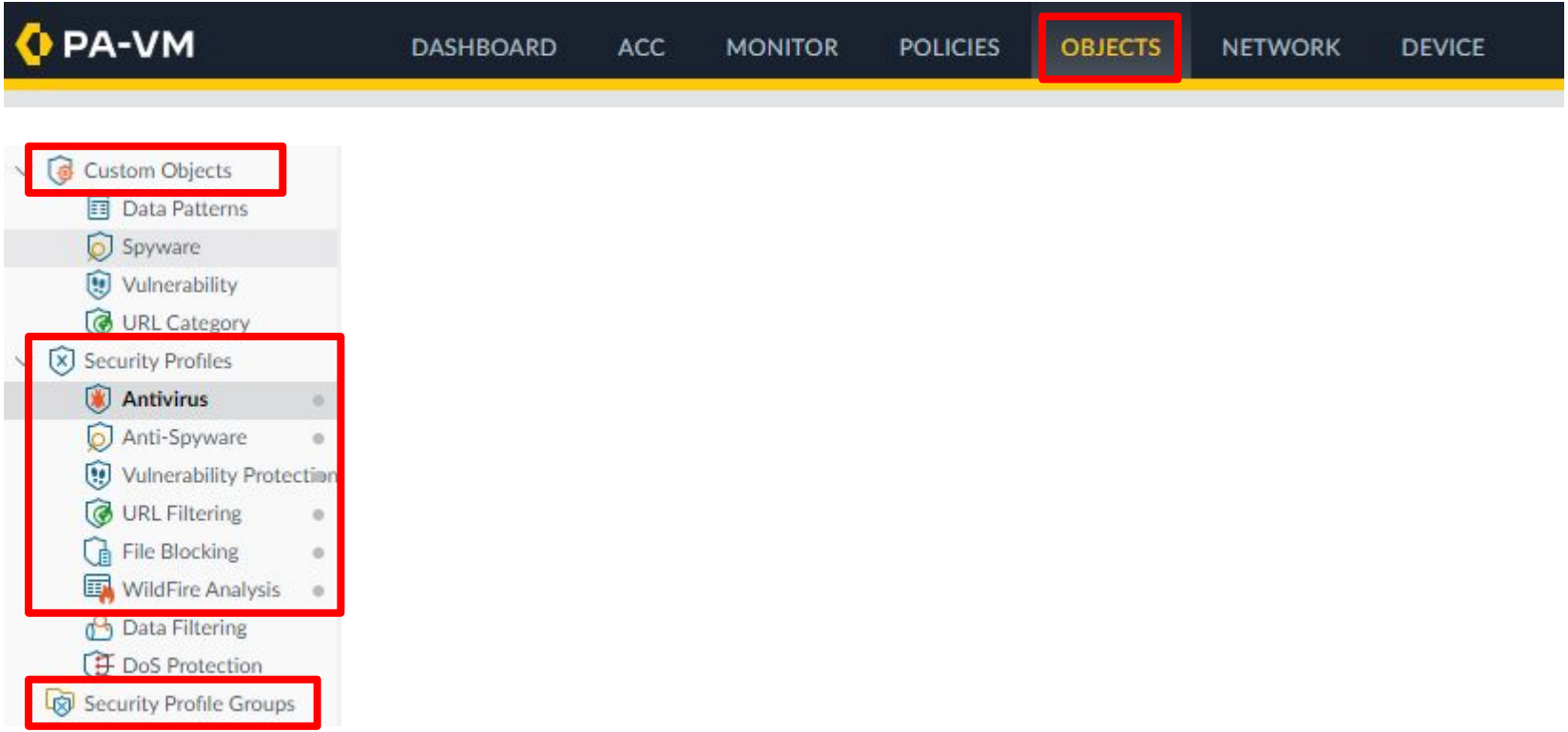
Licenses

Licenses:





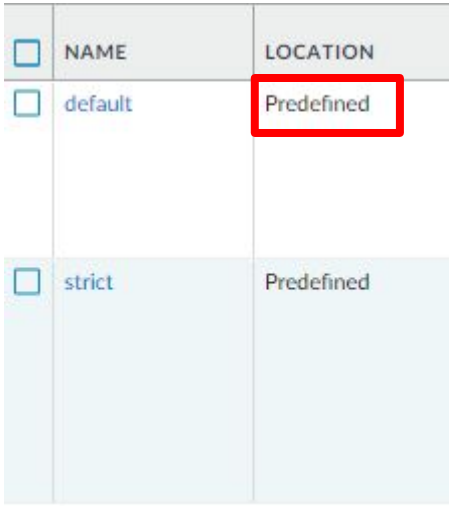
Profiles



Profiles

Security Profiles:

- Predefined rules cannot be modified or deleted.
- Rules can be cloned as a starting point for a new custom profile.
- Create a custom profile from scratch.



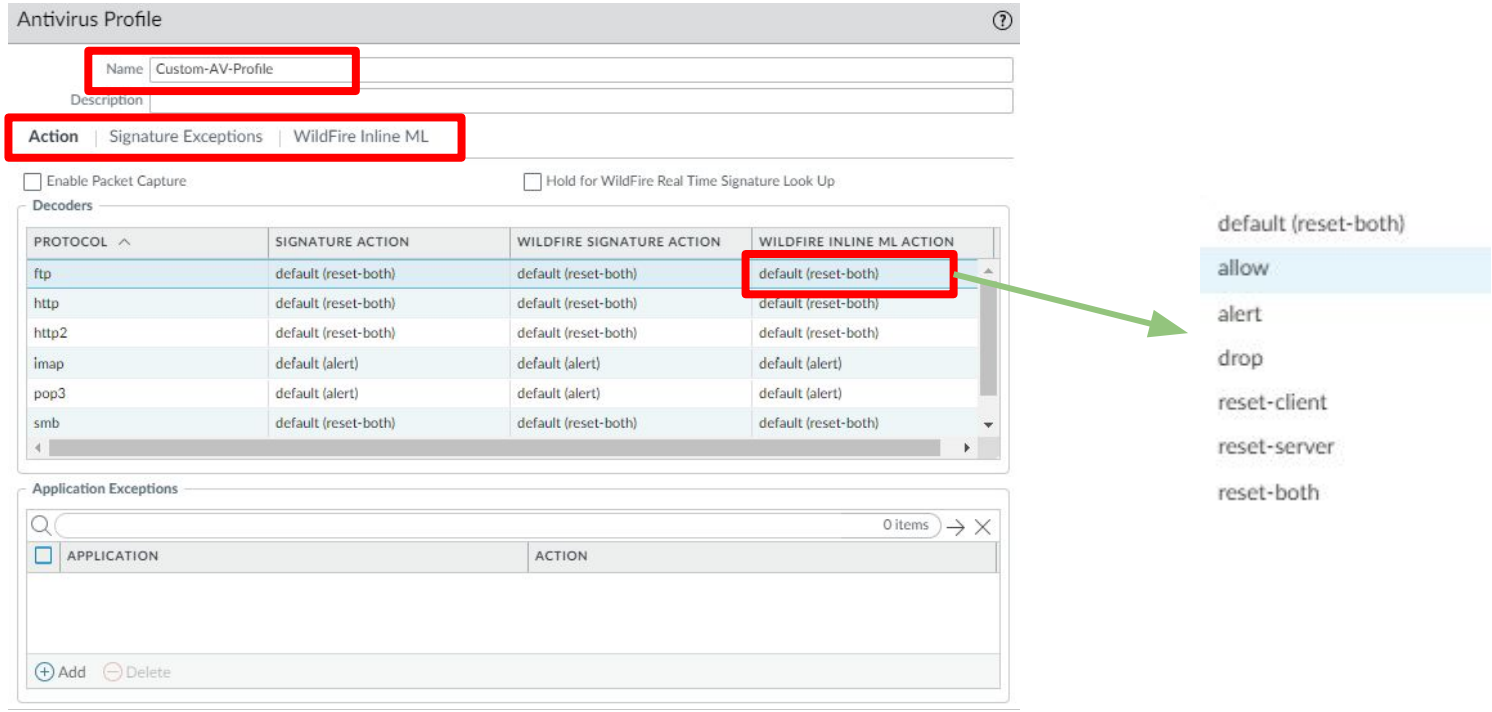
Profiles

AntiVirus (ATP): Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads.

NAME	LOCATION	PACKET CAPTURE	HOLD MODE	Decoders			
				PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
default	Predefined			http	default (reset-both)	default (reset-both)	default (reset-both)
				http2	default (reset-both)	default (reset-both)	default (reset-both)
				smtp	default (alert)	default (alert)	default (alert)
				imap	default (alert)	default (alert)	default (alert)
				pop3	default (alert)	default (alert)	default (alert)
				ftp	default (reset-both)	default (reset-both)	default (reset-both)
				smb	default (reset-both)	default (reset-both)	default (reset-both)

Profiles

AntiVirus (ATP):



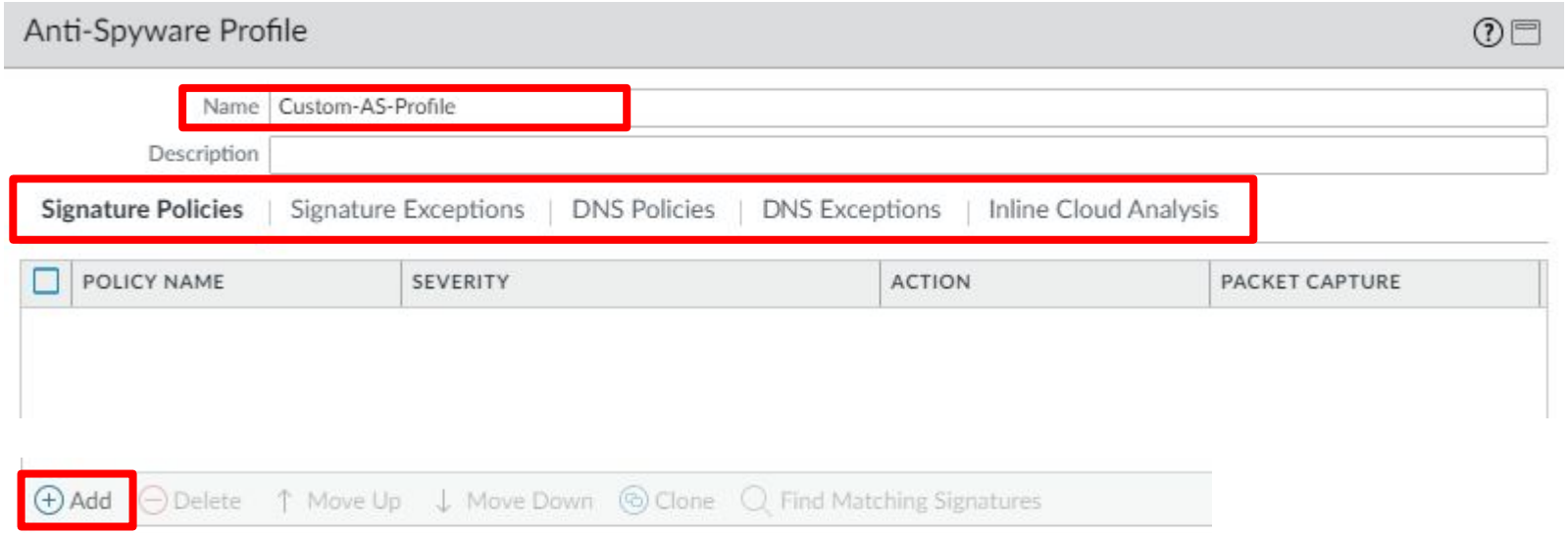
Profiles

AntiSpyware (ATP): Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.

NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable

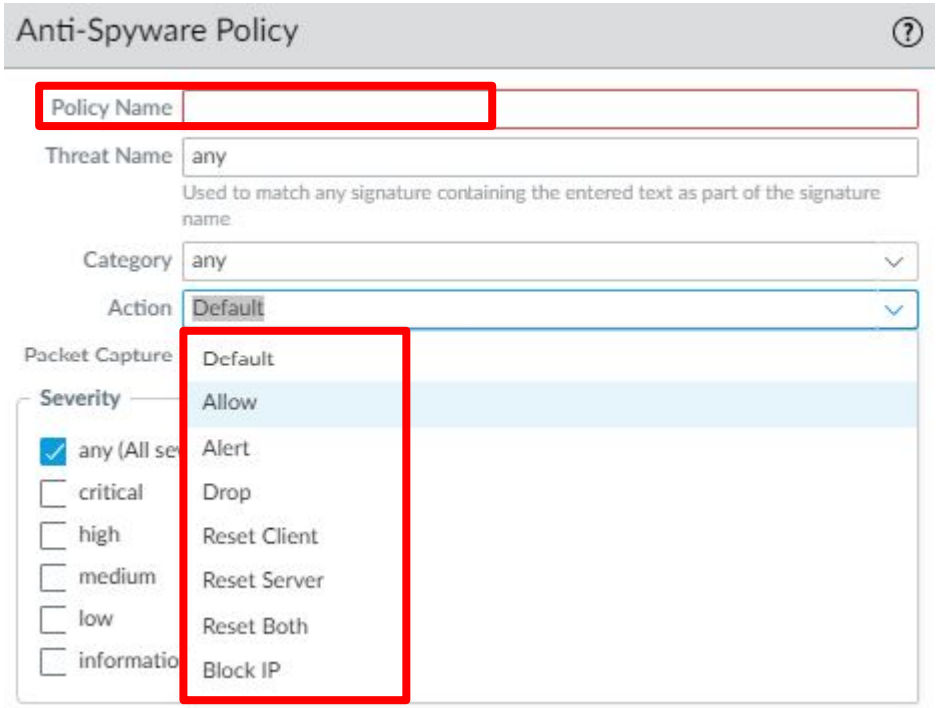
Profiles

AntiSpyware (ATP): Custom



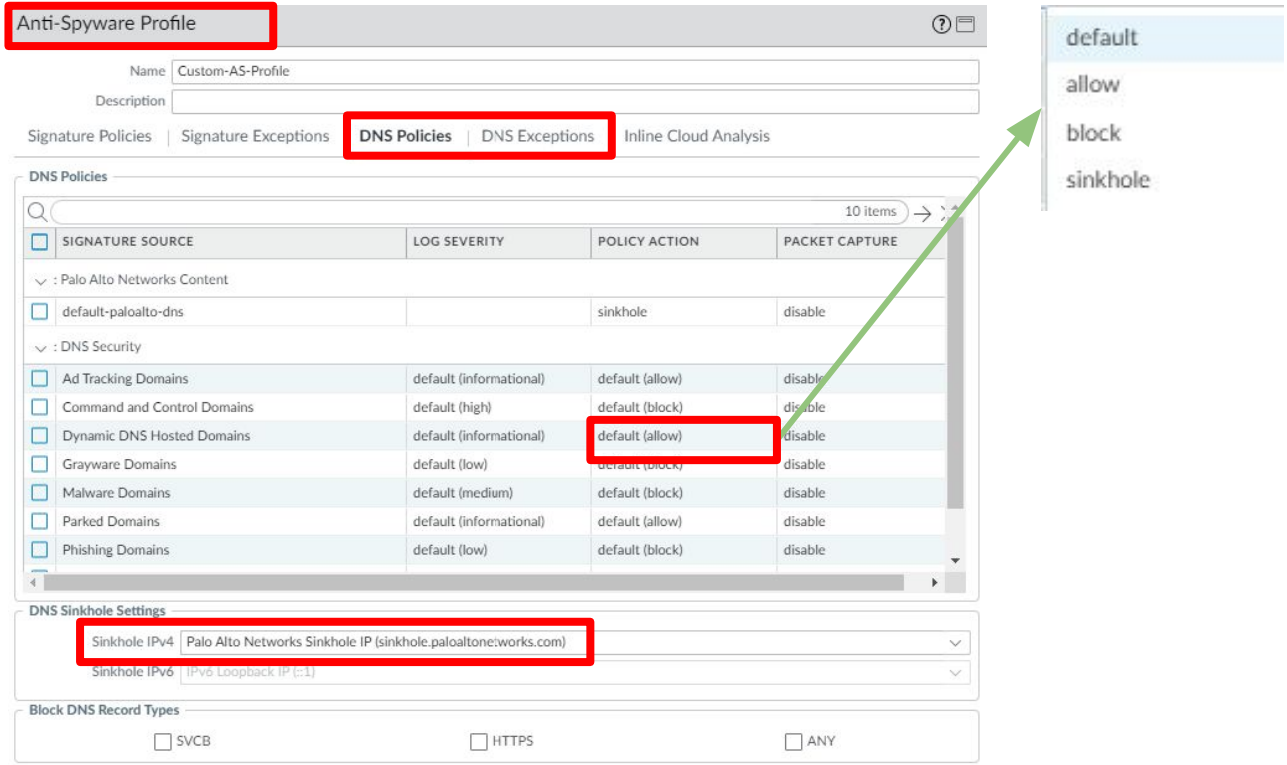
Profiles

AntiSpyware (ATP): Custom



Profiles

DNS Security: (ATP and DNS)



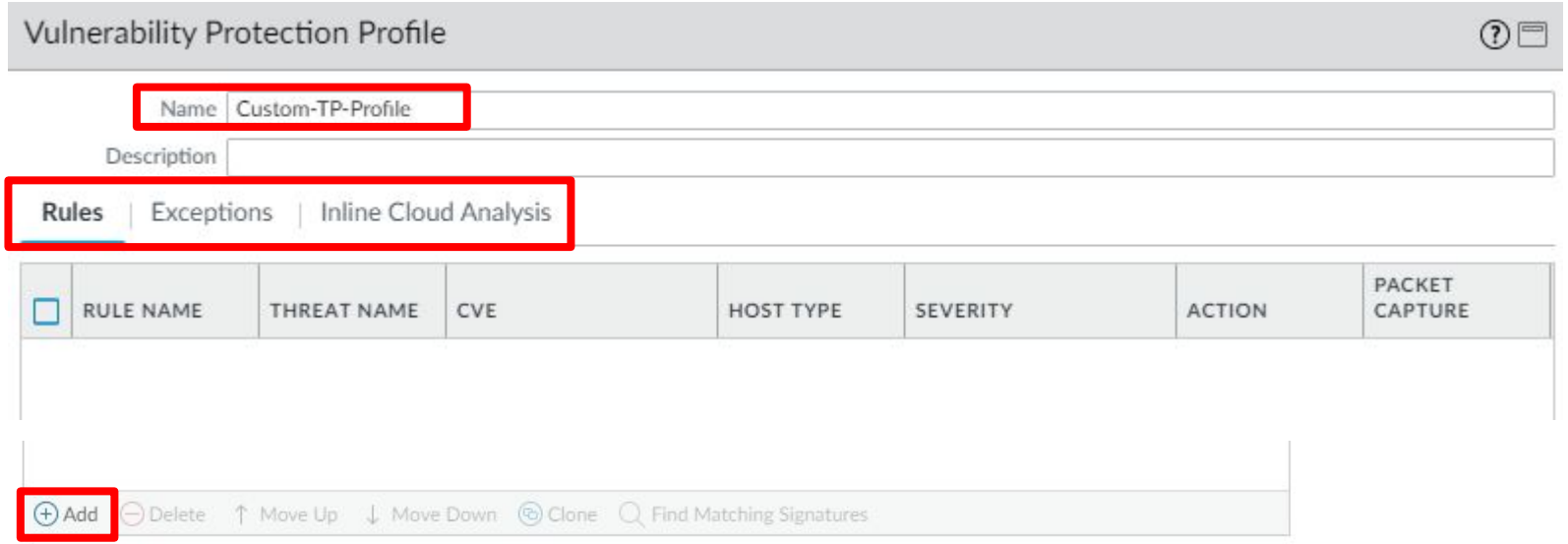
Profiles

Vulnerability Protection (ATP): Vulnerability Protection profiles stop attempts to exploit system flaws or gain unauthorized access to systems. While Anti-Spyware profiles help identify infected hosts as traffic leaves the network, Vulnerability Protection profiles protect against threats entering the network.

NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable

Profiles

Vulnerability Protection (ATP): Custom



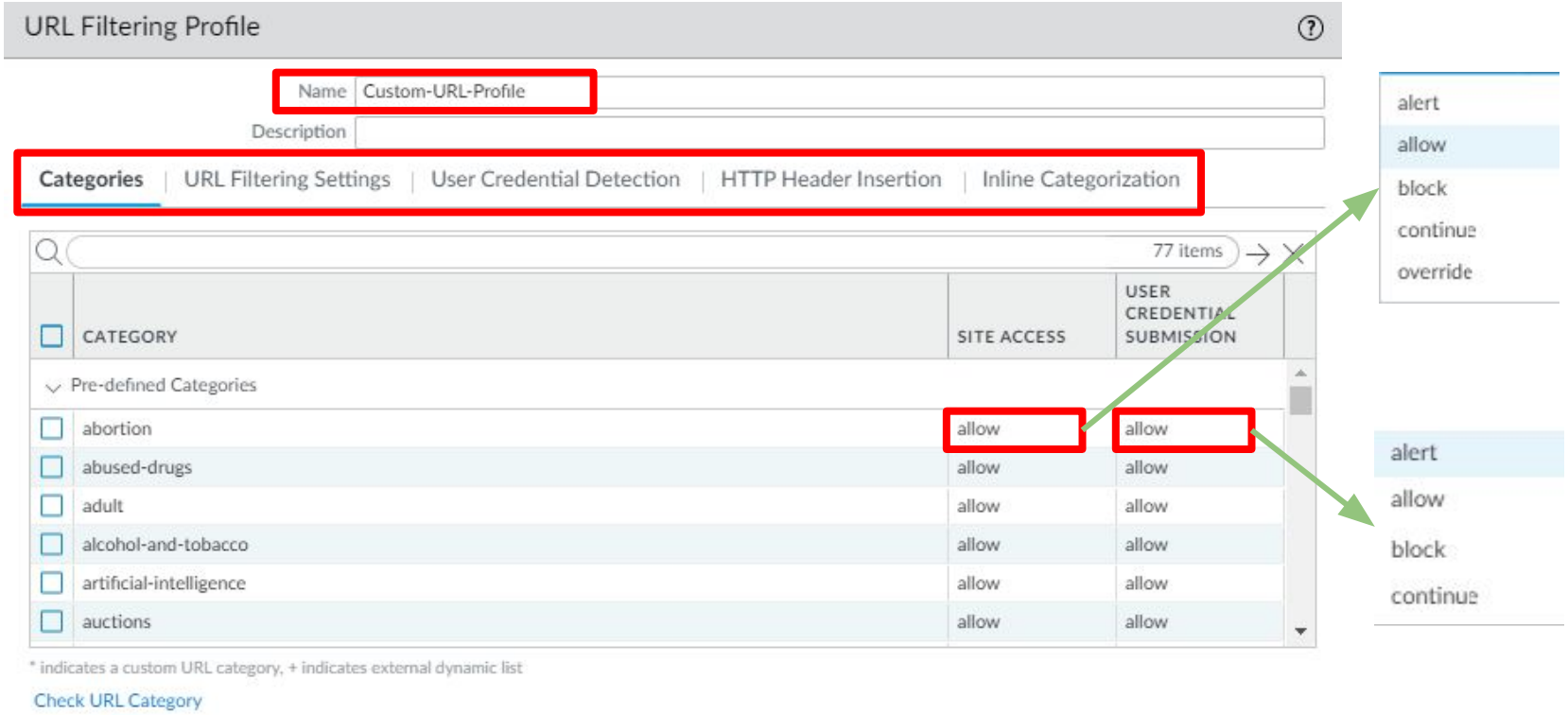
Profiles

Advanced URL Filtering: URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS.URL Filtering profiles enable you to monitor and control how users access the web over HTTP and HTTPS.

NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION
default	Predefined	Allow Categories (59) Alert Categories (6) Continue Categories (0) Block Categories (12) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)

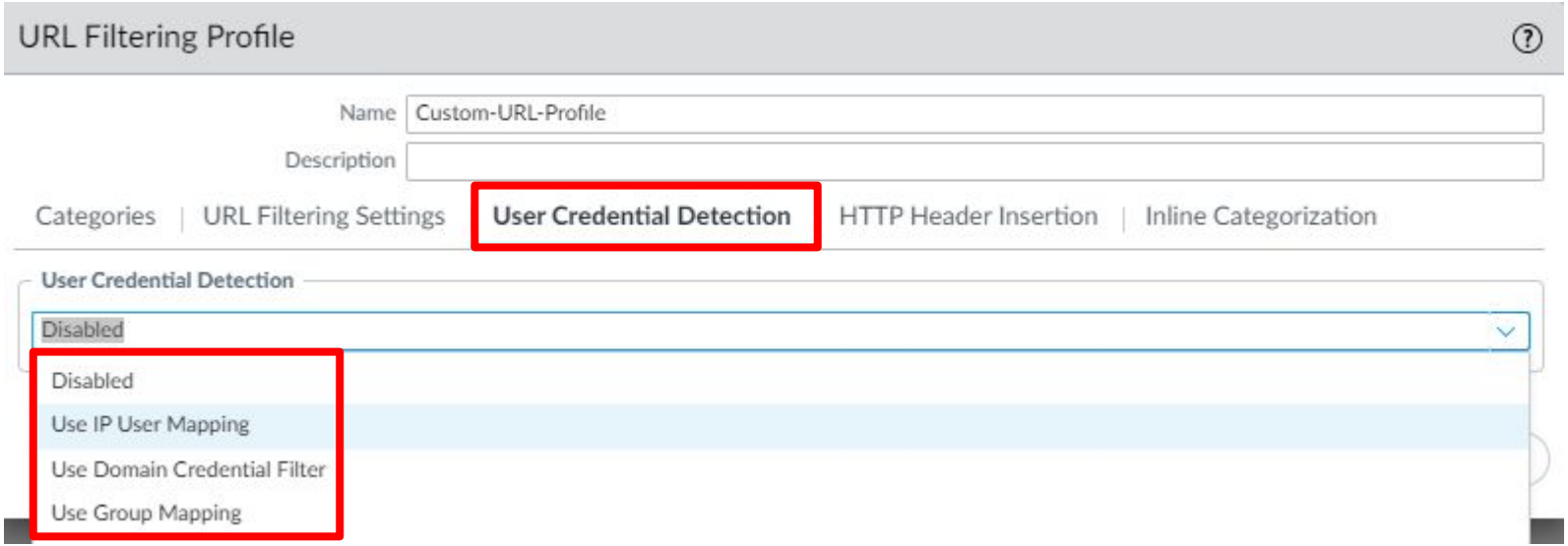
Profiles

URL Filtering: Custom



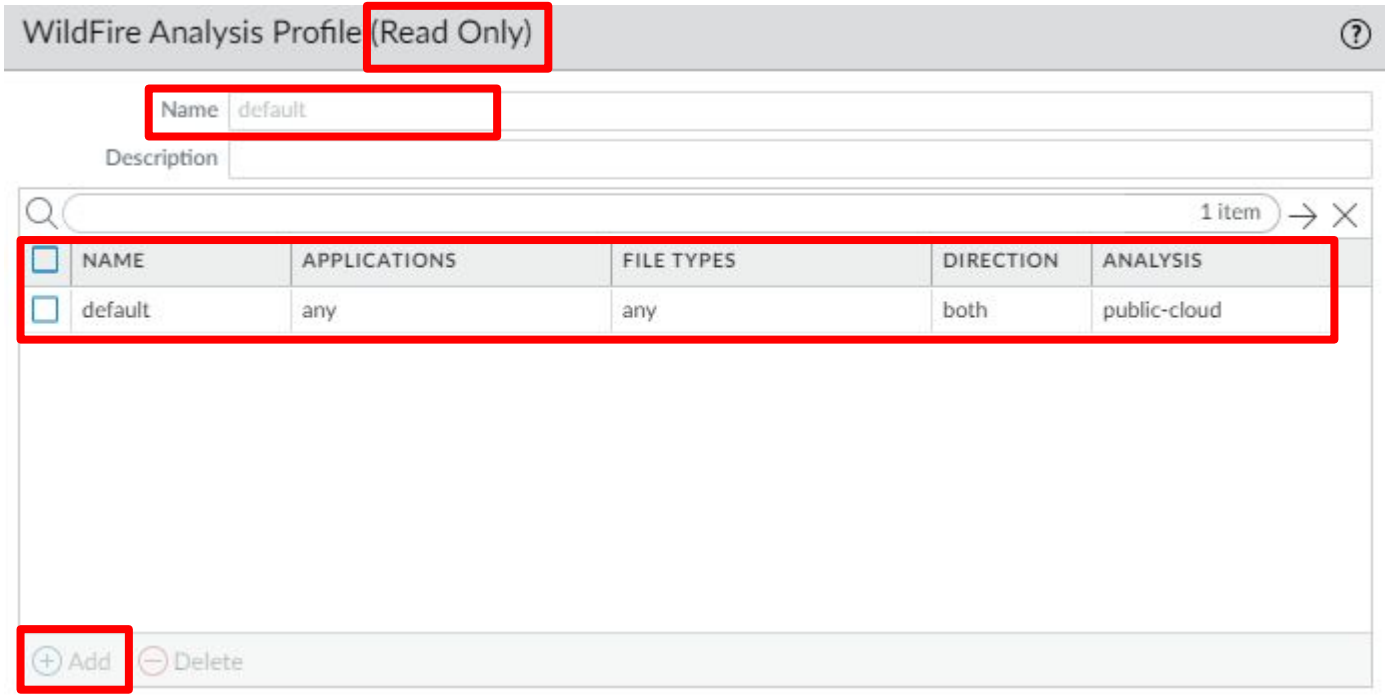
Profiles

URL Filtering: Credential Theft Prevention - USER-ID Required



Profiles

Advanced WildFire: Use a WildFire analysis profile to enable forwarding of unknown files or email links for WildFire analysis.



Profiles

File Blocking Profile:

- Blocks upload and download of PE files (.scr, .cpl, .dll, .ocx, .pif, .exe), Java files (.class, .jar), Help files (.chm, .hlp) and other potentially malicious file types, including .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat.

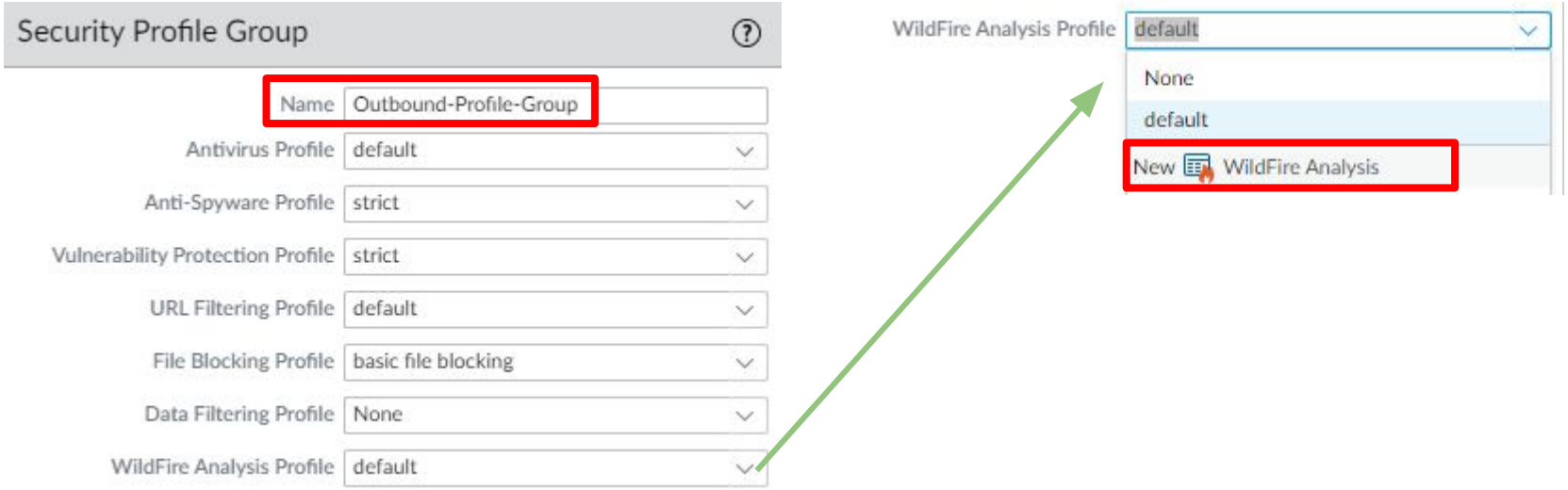
NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip
		Log all other file types	any	any

- Blocks the same file types as the other profile, and additionally blocks flash, .tar, multi-level encoding, .cab, .msi, encrypted-rar, and encrypted-zip files.

strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf
		Block encrypted files	any	encrypted-rar, encrypted-zip
		Log all other file types	any	any

Profiles

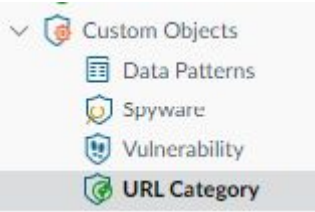
Security Profile Groups:



Profiles

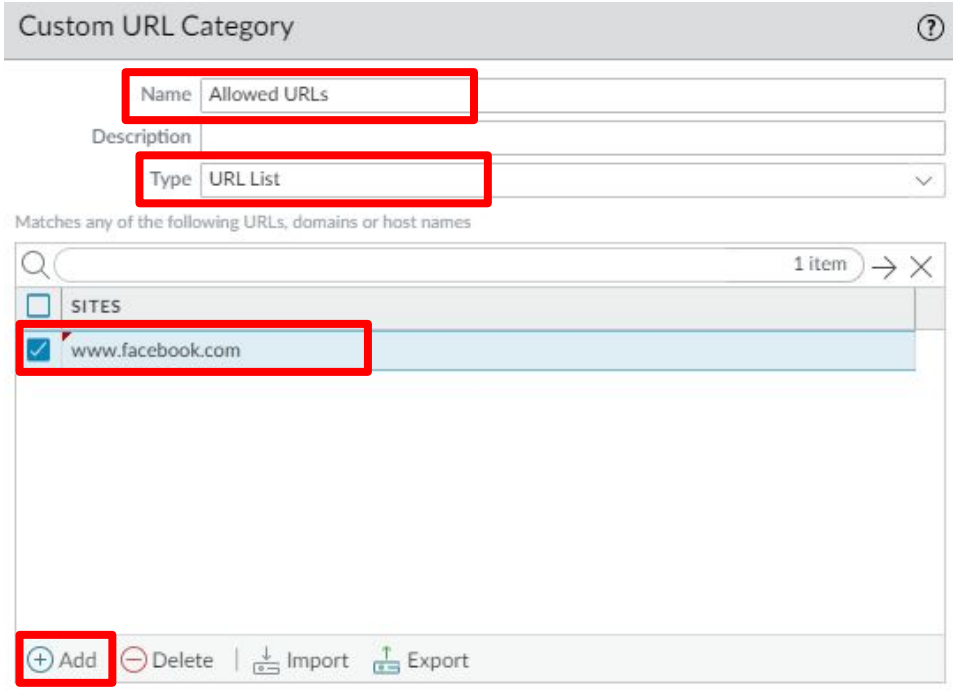
Custom Objects:

- Data Patterns - Defines patterns used in Data Filtering profile
- Spyware - Create custom signatures to use in a AS profile
- Vulnerability - Create custom signatures to use in a VP profile
- URL Category - Create custom URL categories to use in a URL Filtering profile



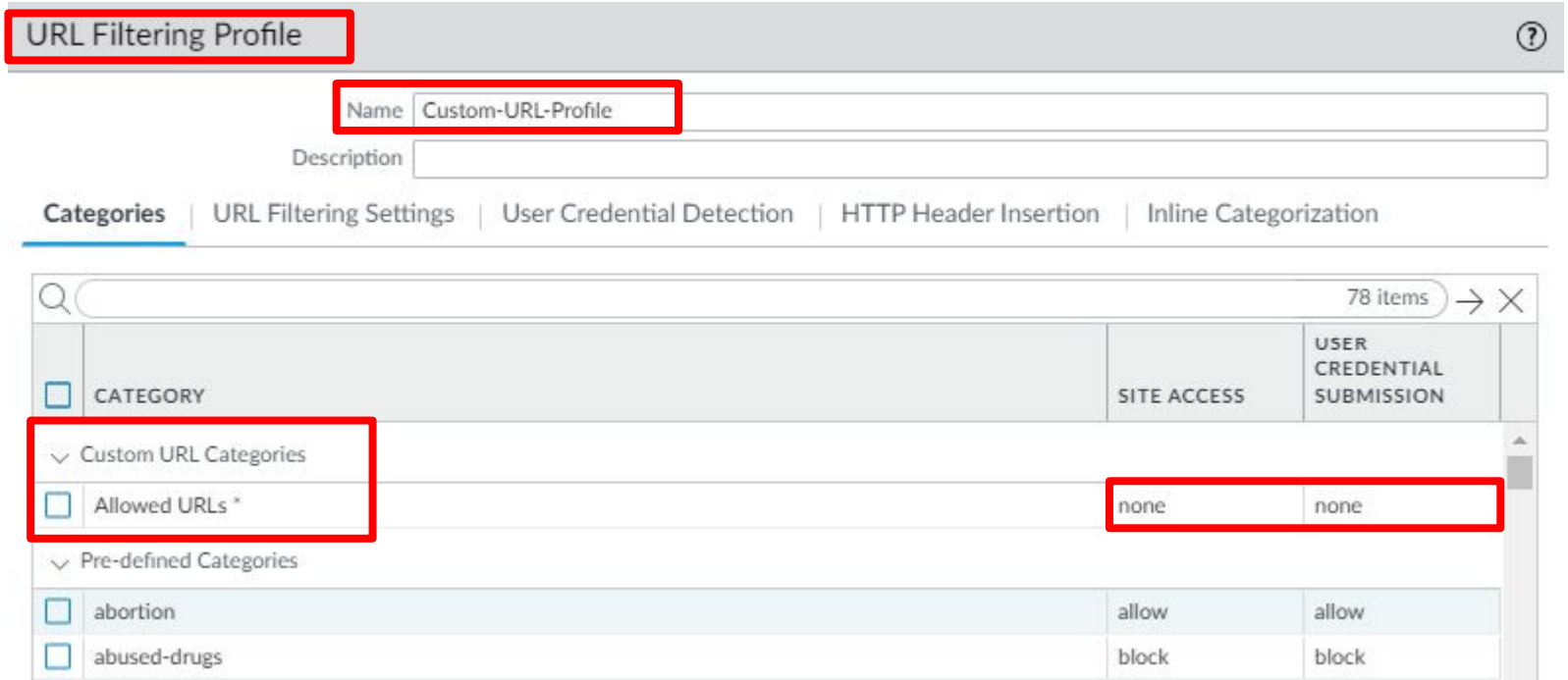
Profiles

Custom Objects: URL Category



Profiles

Custom Object: URL Category (Automatically added to a custom profile)

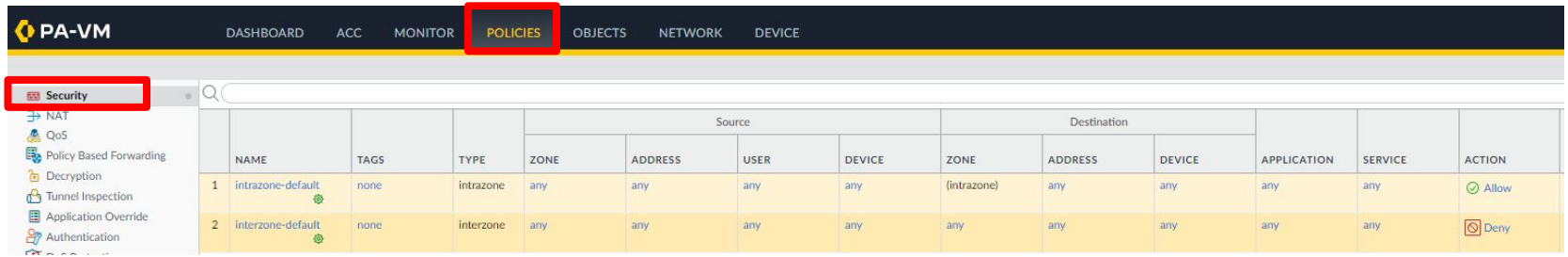


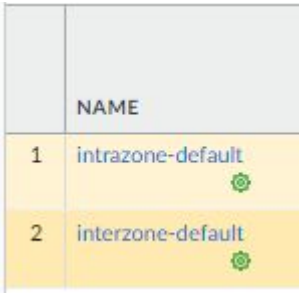
Security Policies

Security Policies

Security Policies:

- Only intrazone traffic is allowed by default.
- All other traffic is denied.





Security Policies

Parts of a rule:

- Required
  - Name
  - Rule Type
  - Source Zone
  - Destination Zone
  - Application
  - Action
- Optional
  - Tag
  - Description
  - Source Address
  - Destination Address
  - URL / URL Category
  - Service
  - Security Profile
  - Options

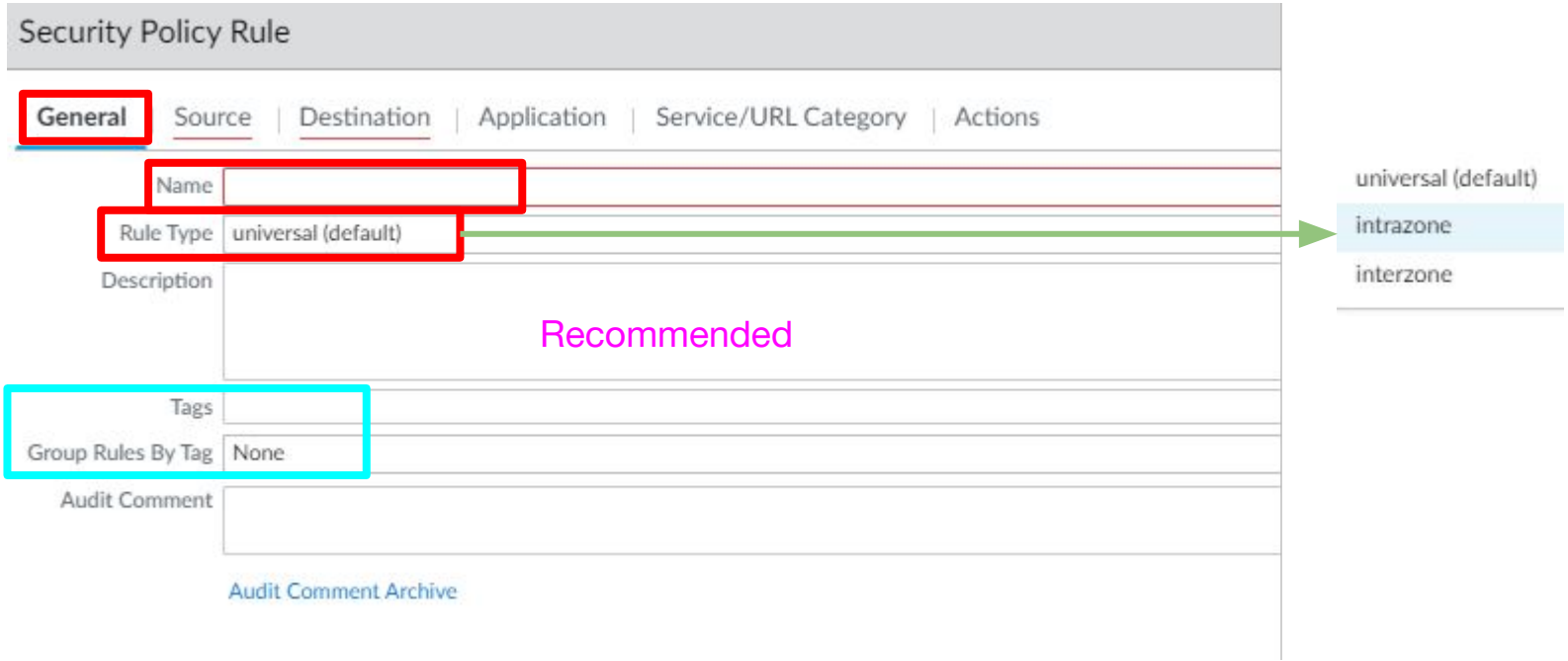
Security Policies

Security Policy Actions:

ACTION	DESCRIPTION
Allow (default)	Allows the traffic.
Deny	Blocks traffic and enforces the default `Deny Action` defined for the application that is being denied.
Drop	Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset isn't sent to the host/application. For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: **Drop** and enable the **Send ICMP Unreachable** check box. When enabled, the ICMP code is sent for `communication with the destination is administratively prohibited`—ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.
Reset client	Sends a TCP reset to the client-side device.
Reset server	Sends a TCP reset to the server-side device.
Reset both	Sends a TCP reset to both the client-side and server-side devices.

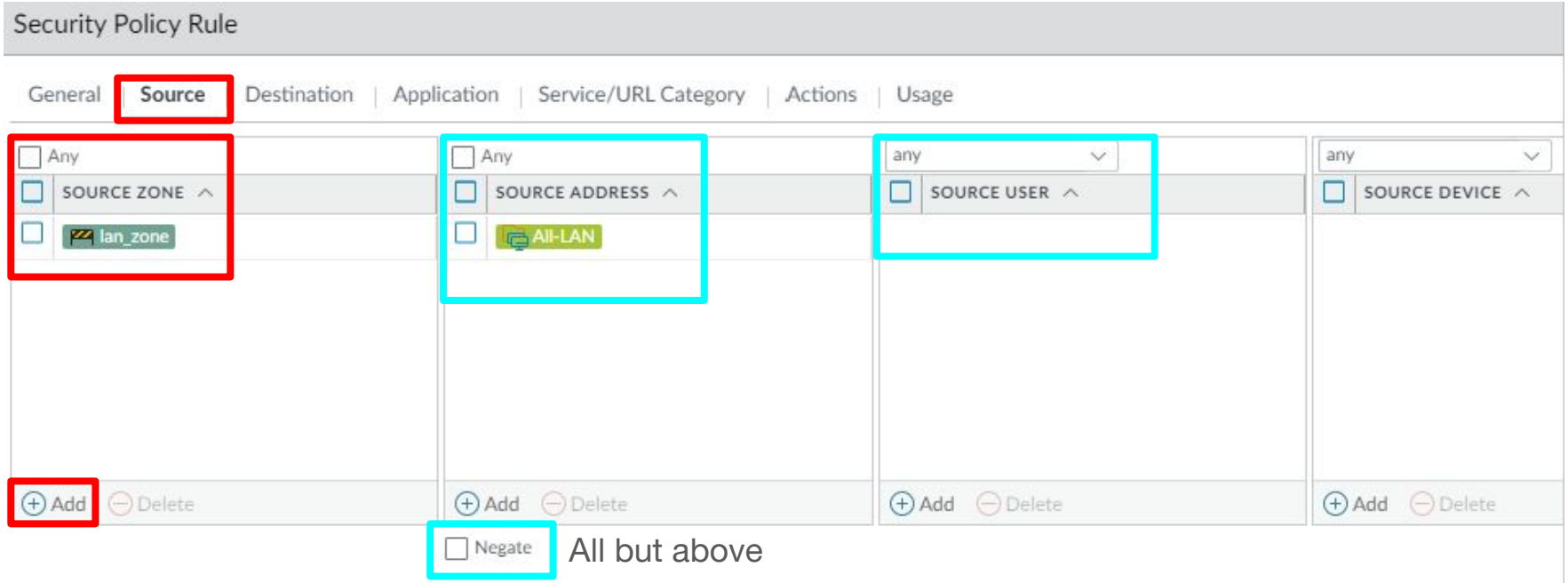
Security Policies

Create a new policy:



Security Policies

Create a new policy:

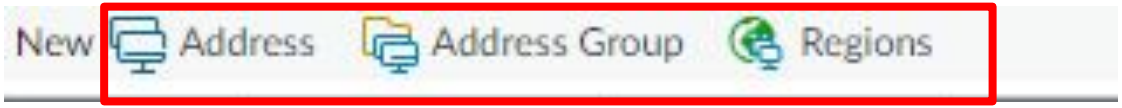


All but above

Security Policies

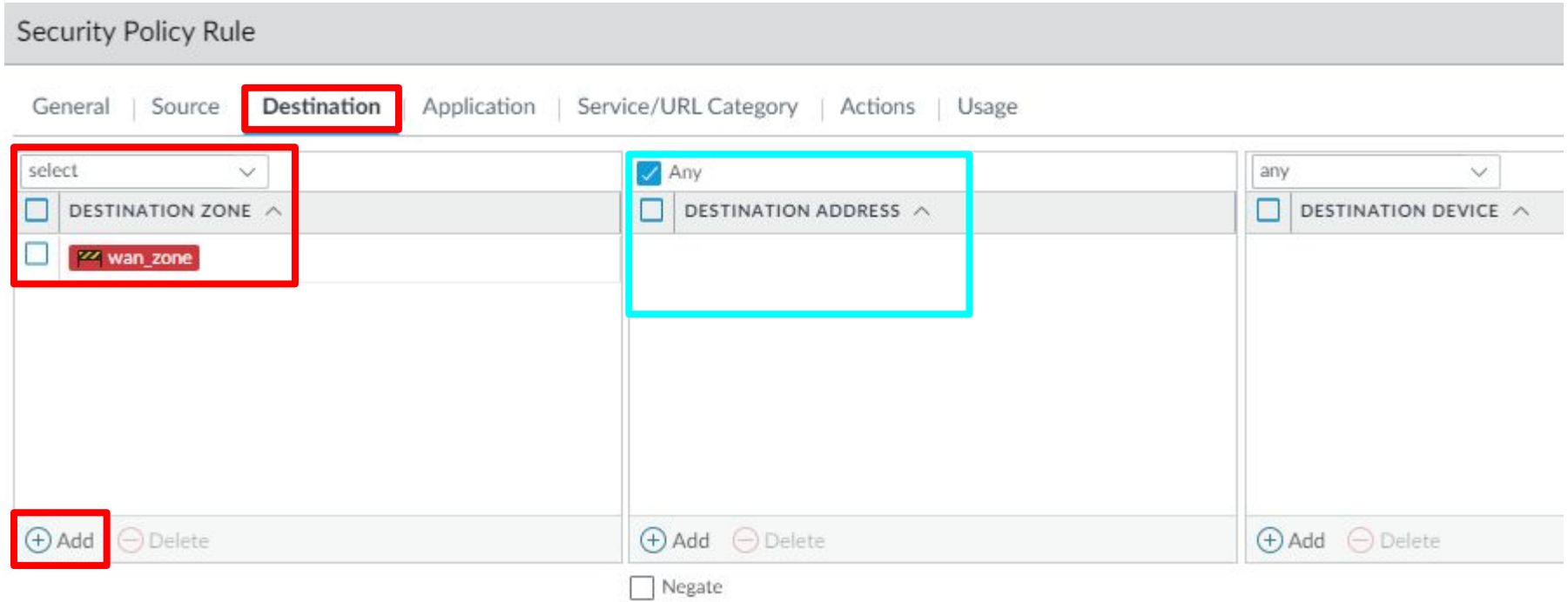
Address Options:

- Address
- Address Group
- External Dynamic List
- Region
  - Predefined - China (CN)
  - Custom



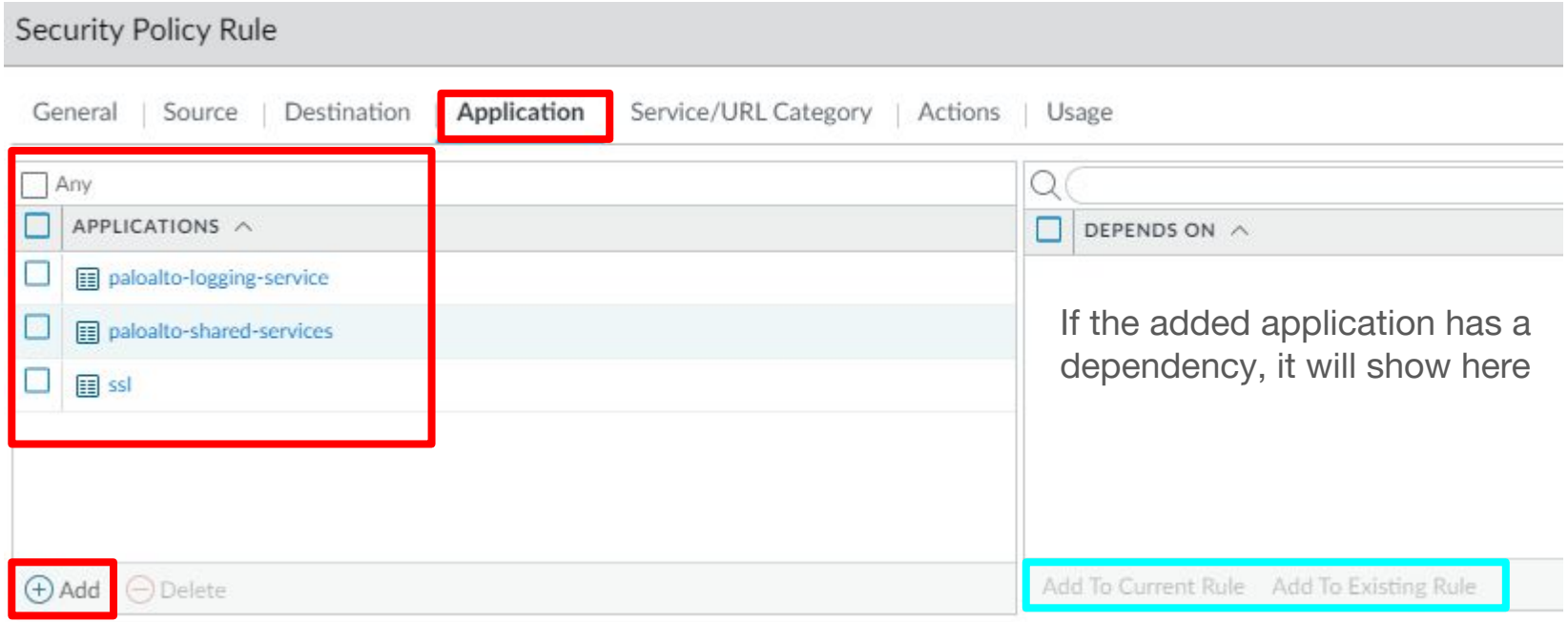
Security Policies

Create a new policy:



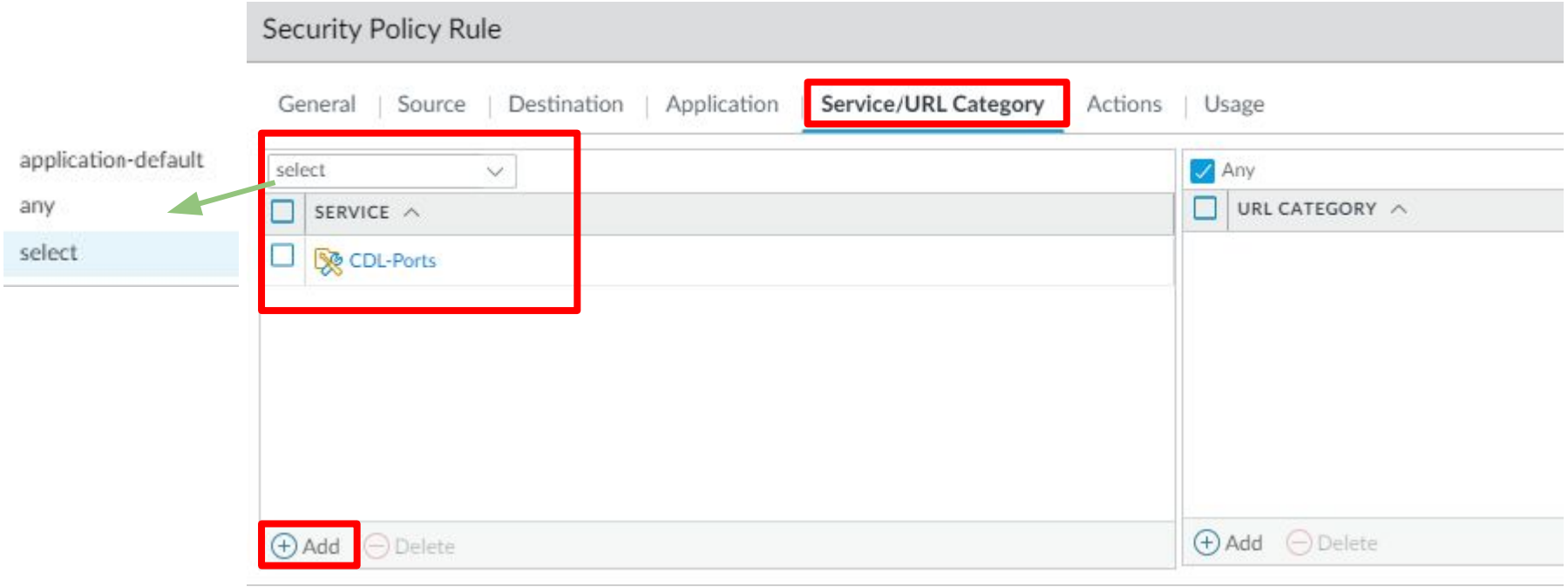
Security Policies

Create a new policy:



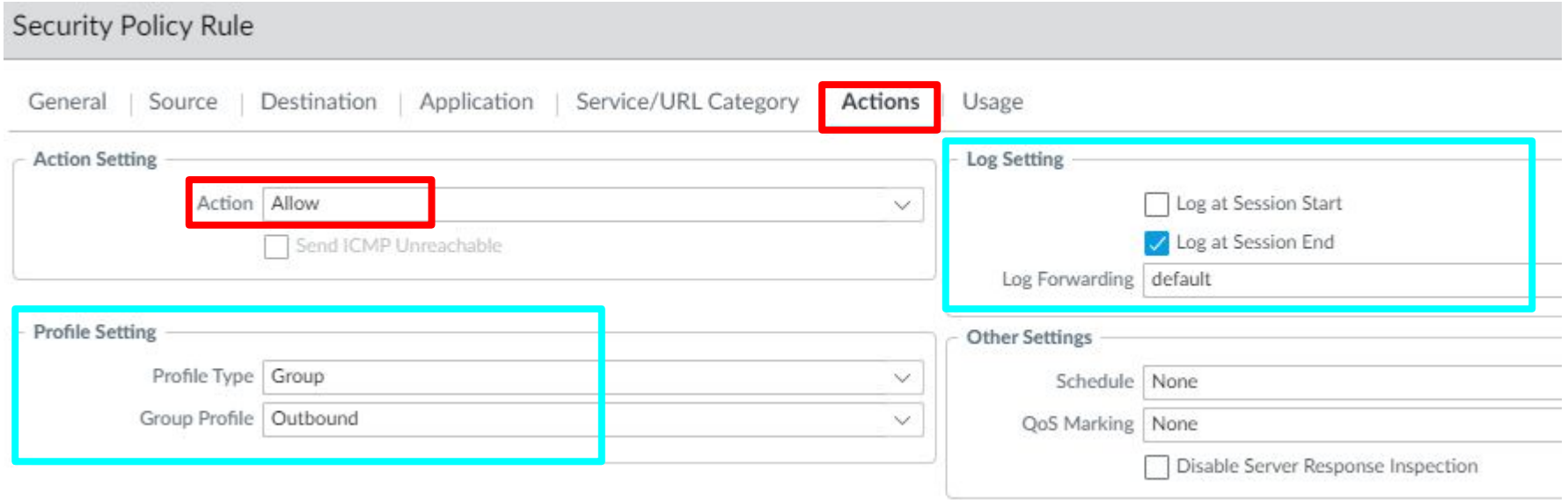
Security Policies

Create a new policy:



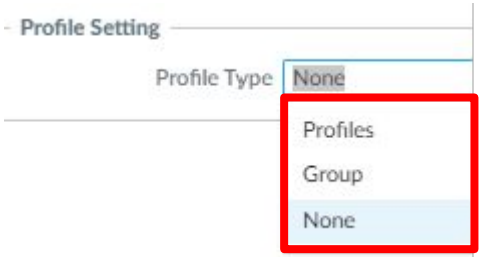
Security Policies

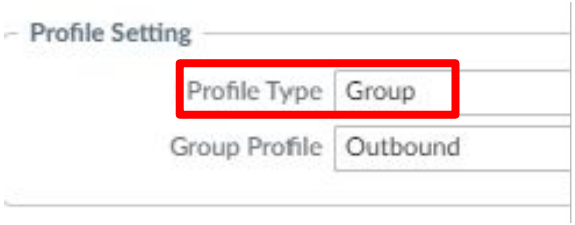
Create a new policy:

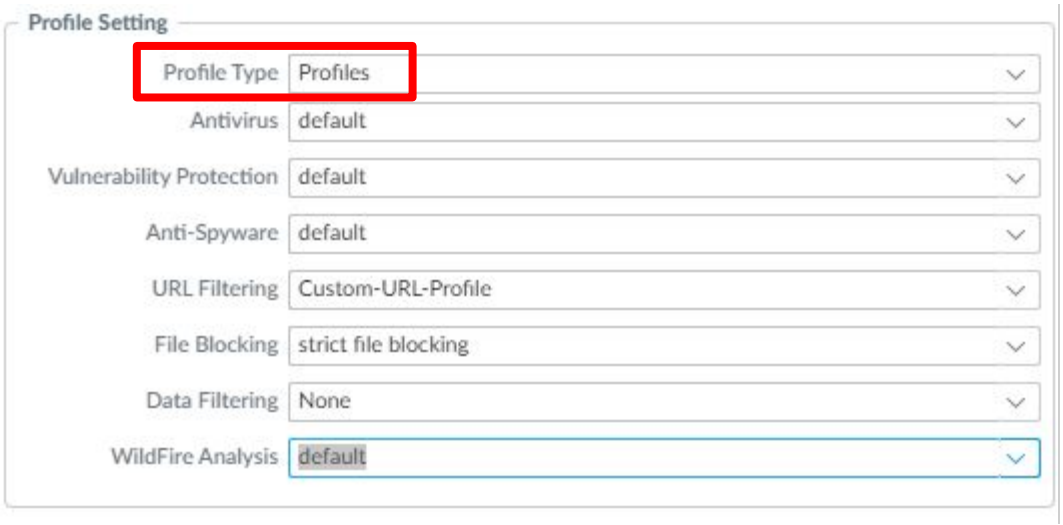


Security Policies

Create a new policy: Profile Settings

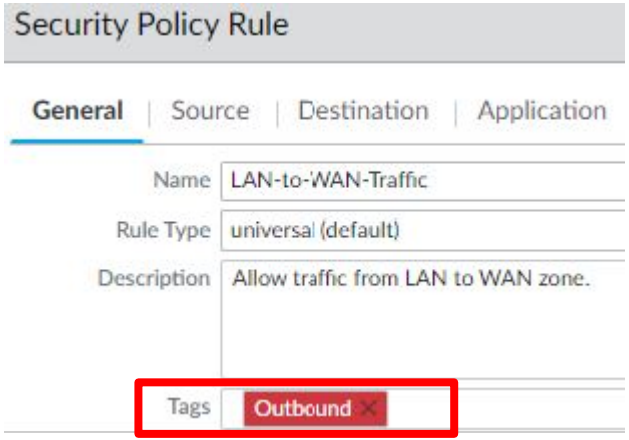






Security Policies

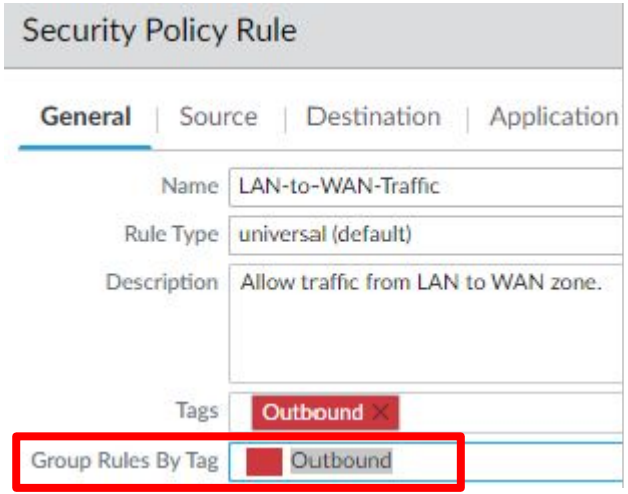
Policies: Using Tags

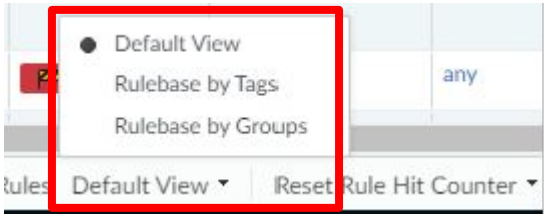


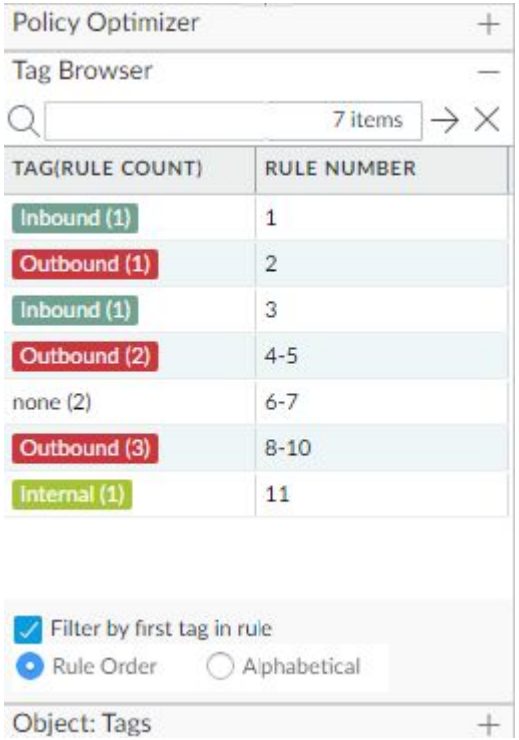
5	Block-Google-QUIC	Outbound	universal	any	any
6	Block WAN to WAN ...	none	universal	wan_zone	any
7	*Rule for Exam*	*none*	*universal*	*lan_zone*	10.0.40.103
8	Allow Traffic to CDL	Outbound	universal	lan_zone	Data
9	Email_Rule	Outbound	universal	lan_zone	All-LAN
10	LAN-to-WAN-Traffic	Outbound	universal	lan_zone	All-LAN
11	Internal_Traffic	Internal	universal	lan_zone	All-LAN

Security Policies

Policies: Grouping







Security Policies

Policy Options:

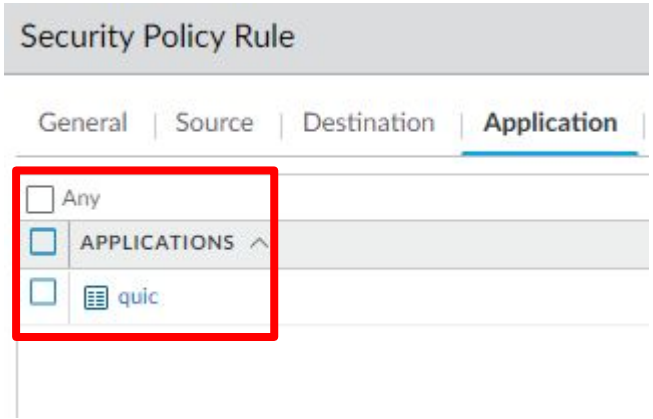
Security Policies

Recommended Block Rules:

				Source			Destination	
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	Geo-Block-Inbound	Inbound	universal	any	CN IR KP RU	any	any	any	any
2	Geo-Block-Outbound	Outbound	universal	any	any	any	any	any	CN IR KP RU
3	Known-Bad-EDL-Inb...	Inbound	universal	any	Palo Alto Networks - Bulletproo... Palo Alto Networks - High risk I... Palo Alto Networks - Known ma... Palo Alto Networks - Tor exit IP ...	any	any	any	any
4	Known-Bad-EDL-Ou...	Outbound	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP a... Palo Alto Networks - High risk IP ad... Palo Alto Networks - Known malicio... Palo Alto Networks - Tor exit IP addr...

Security Policies

Recommended Block Rules:



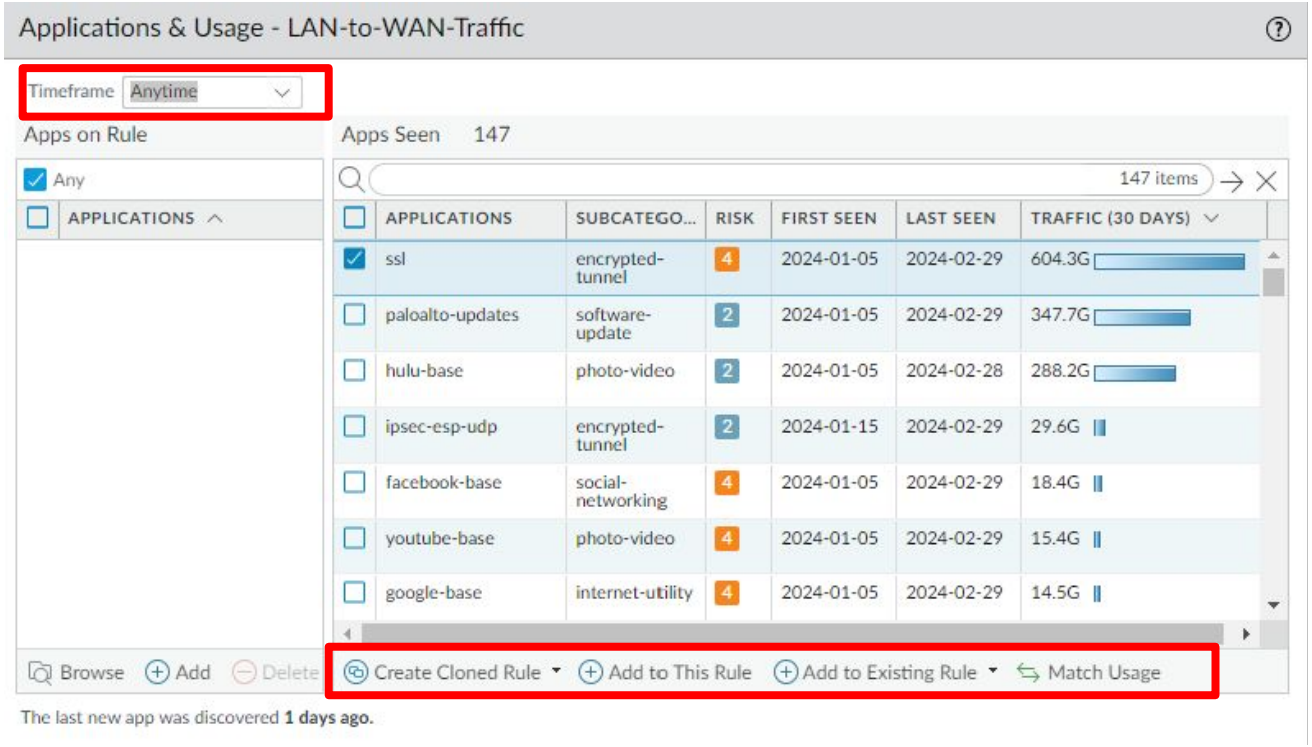
Security Policies

Rule Usage:

Rule Usage				DAYS WITH NO NEW APPS	MODIFIED	CREATED
HIT COUNT	LAST HIT	FIRST HIT	APPS SEEN			
0	-	-	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
113247	2024-02-29 16:26:05	2024-01-05 16:18:21	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
485033	2024-02-29 16:30:53	2024-01-05 18:43:23	-	-	2024-01-05 18:39:30	2024-01-05 18:39:30
949	2024-01-12 17:26:44	2024-01-12 13:52:04	14	48	2024-01-12 17:33:16	2024-01-12 13:51:57
68955	2024-02-29 16:23:03	2024-01-05 17:21:39	3	55	2024-01-05 19:21:39	2024-01-05 17:15:37
19262	2024-02-29 16:18:16	2024-01-05 16:21:03	1	55	2024-01-05 19:21:39	2024-01-04 09:40:36
22519660	2024-02-29 16:31:00	2024-01-05 16:18:30	147	1	2024-01-05 19:21:39	2024-01-04 09:40:36
4019852	2024-02-29 16:31:01	2024-01-05 16:18:29	15	7	2024-01-05 19:21:39	2024-01-04 09:40:36

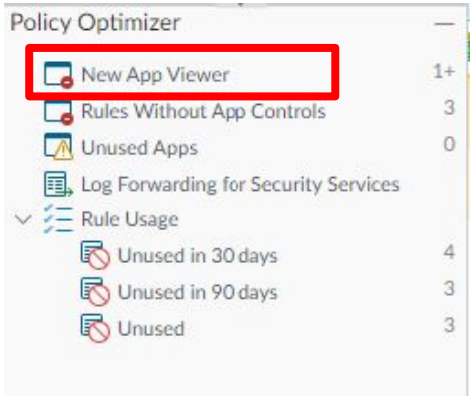
Security Policies

Applications Seen:



Security Policies

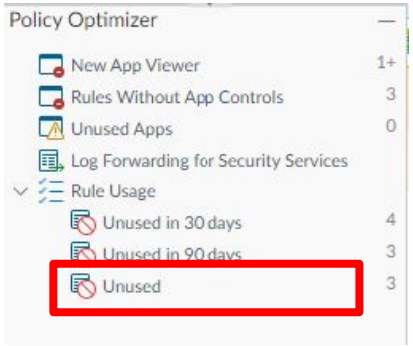
Policy Optimizer:



	NAME	SERVICE	APPLICATION	TRAFFIC (BYTES, 30 DAYS)	App Usage			
					APPS ALLOWED	APPS SEEN	DAYS WITH NO NEW APPS	COMPARE
10	LAN-to-WAN-Traffic	application-...	any	1.4T	any	147	1	Compare
11	Internal_Traffic	application-...	any	1.5G	any	15	7	Compare
7	*Rule for Exam*	*any*	*any*	0	any	14	48	Compare

Security Policies

Policy Optimizer:



Timeframe All time | Usage Unused | Exclude rules reset during the last 90 days

	NAME	Rule Usage HIT COUNT	LAST HIT	FIRST HIT	RESET DATE	MODIFIED	CREATED
4	Known-Bad-EDL-Outbound	0	-	-	-	2024-01-04 09:40:36	2024-01-04 09:40:36
12	intrazone-default	0	-	-	-	2024-01-01 10:14:24	2024-01-01 10:14:24
13	interzone-default	0	-	-	-	2024-01-01 10:14:24	2024-01-01 10:14:24

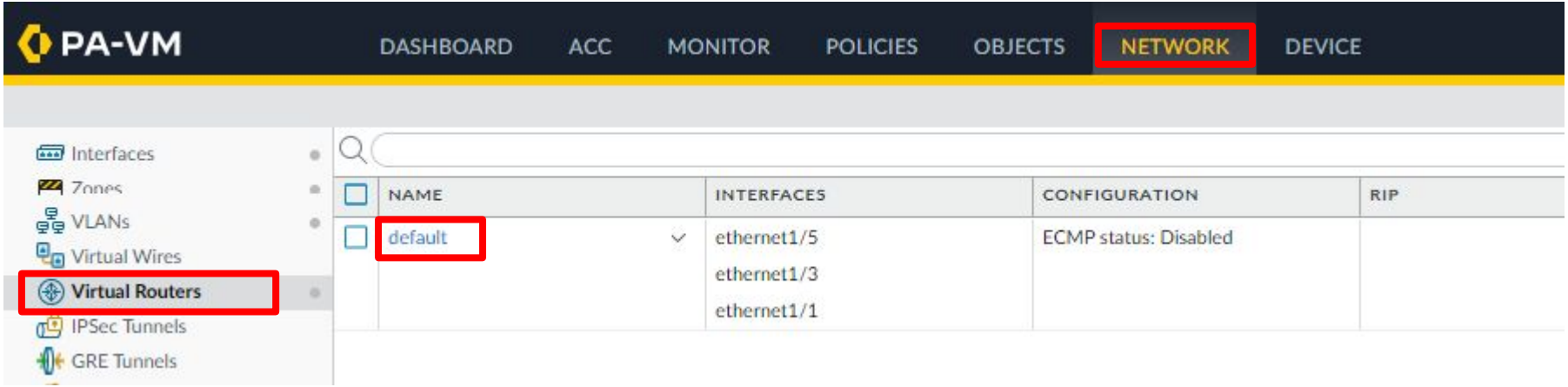
Routing

Routing

Disclaimer:

In this section we will cover the basic configuration of routing for a Palo Alto NGFW firewall. This is a basic configuration class and NOT A ROUTING CLASS! Prior knowledge of basic routing is expected and will be assumed during this section. Configuration of dynamic routing requires matching configurations on both ends of a peering and is outside the scope of this class.

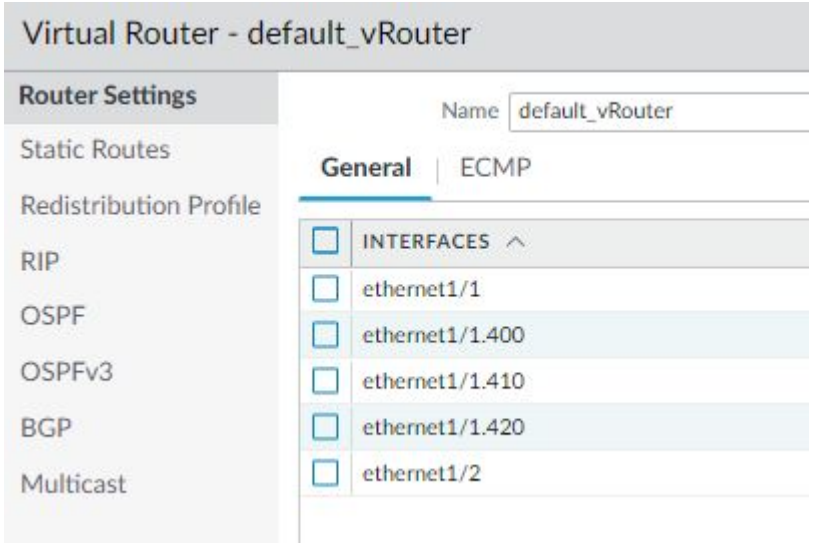
Routing



Routing

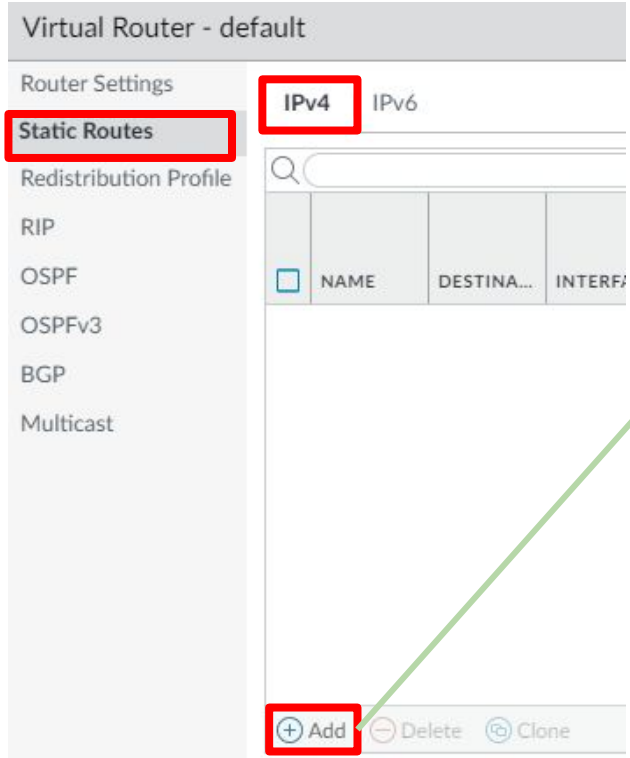
Ways to route traffic:

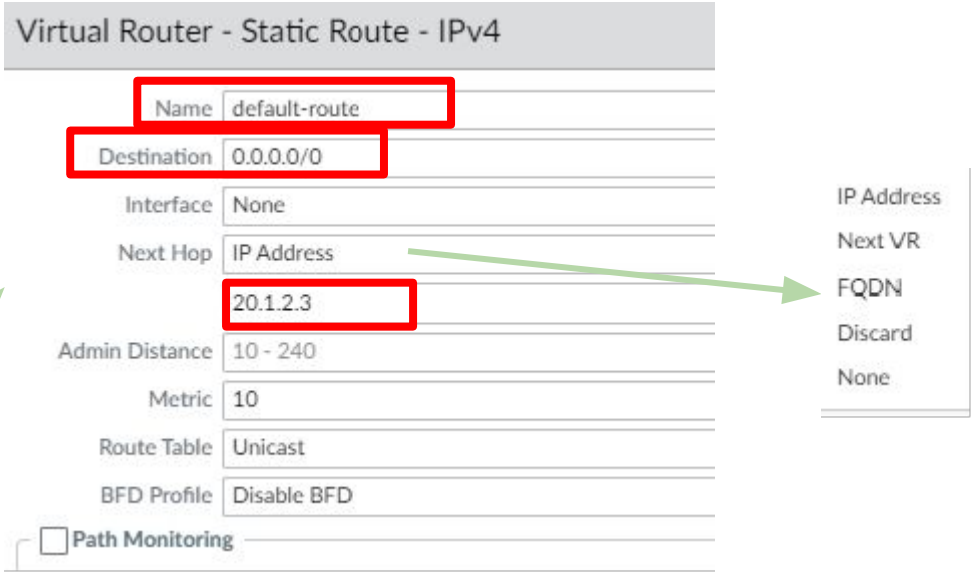
- Static Routing
- Dynamic Routing
  - RIP
  - OSPF
  - OSPFv3
  - BGP
  - Redistribution
- Multicast Routing



Routing

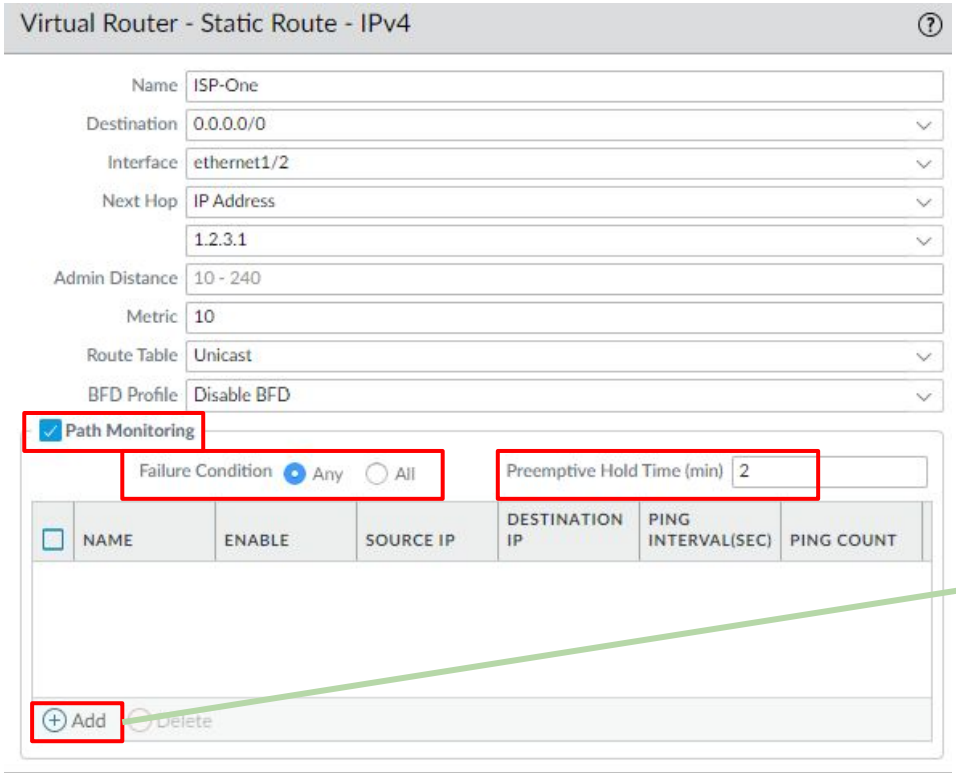
Static Routes:

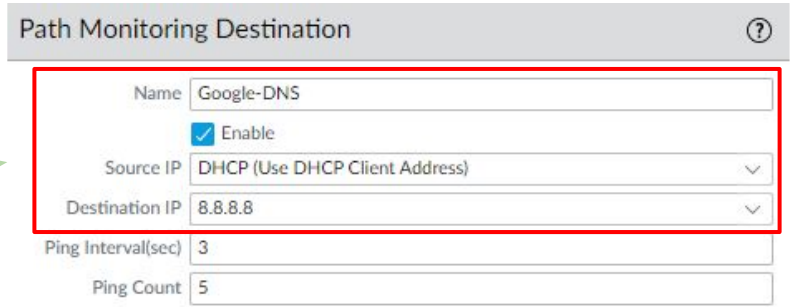




Routing

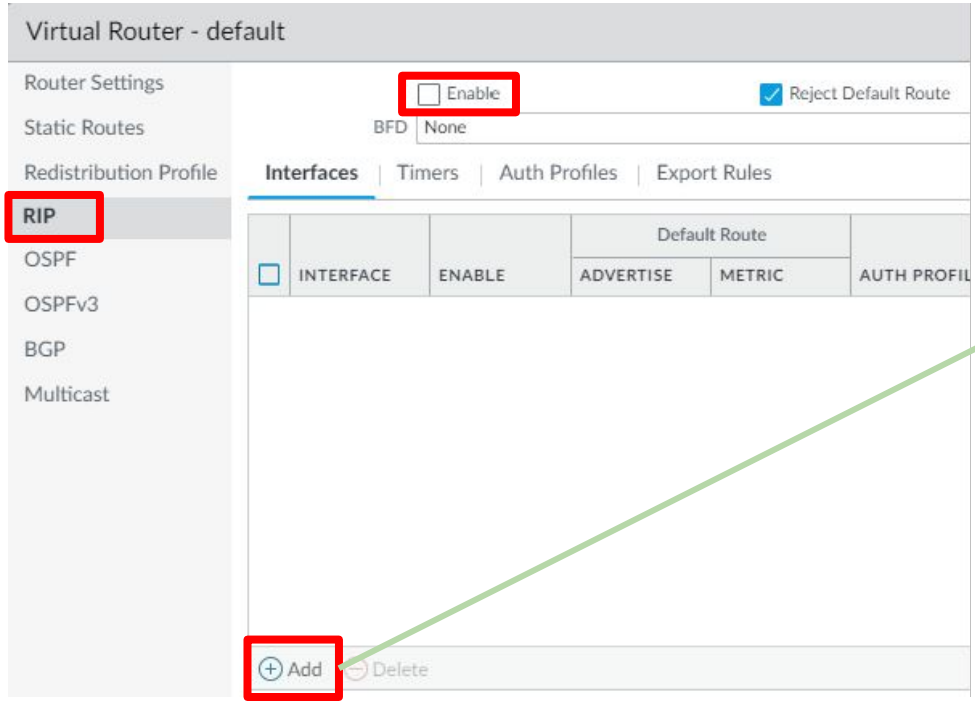
Path Monitoring:

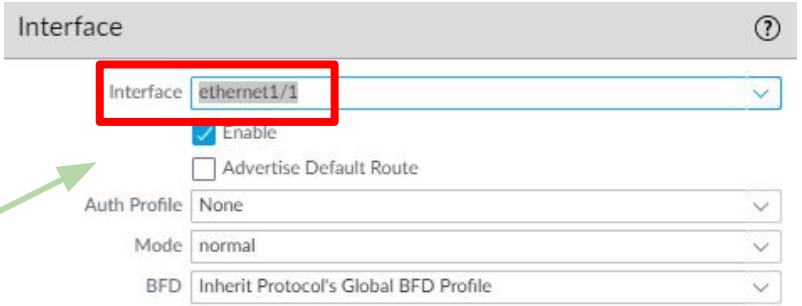




Routing

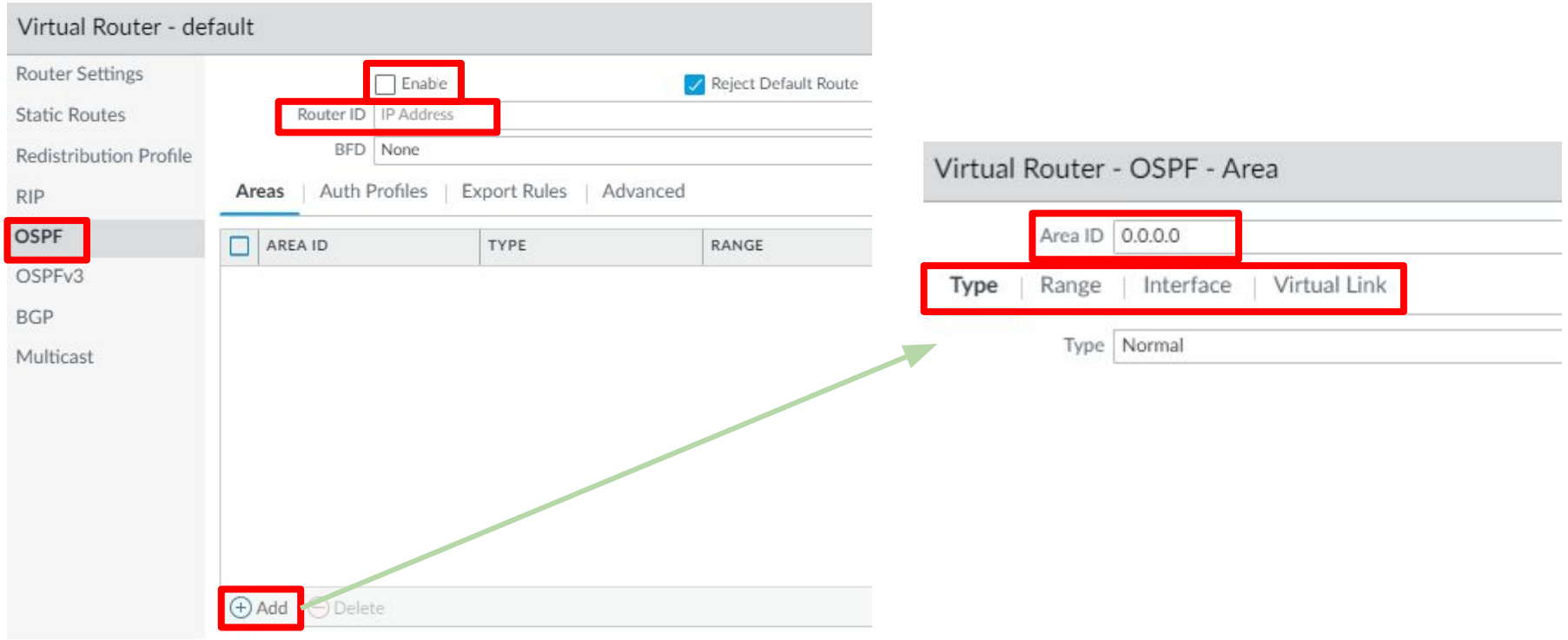
RIP:





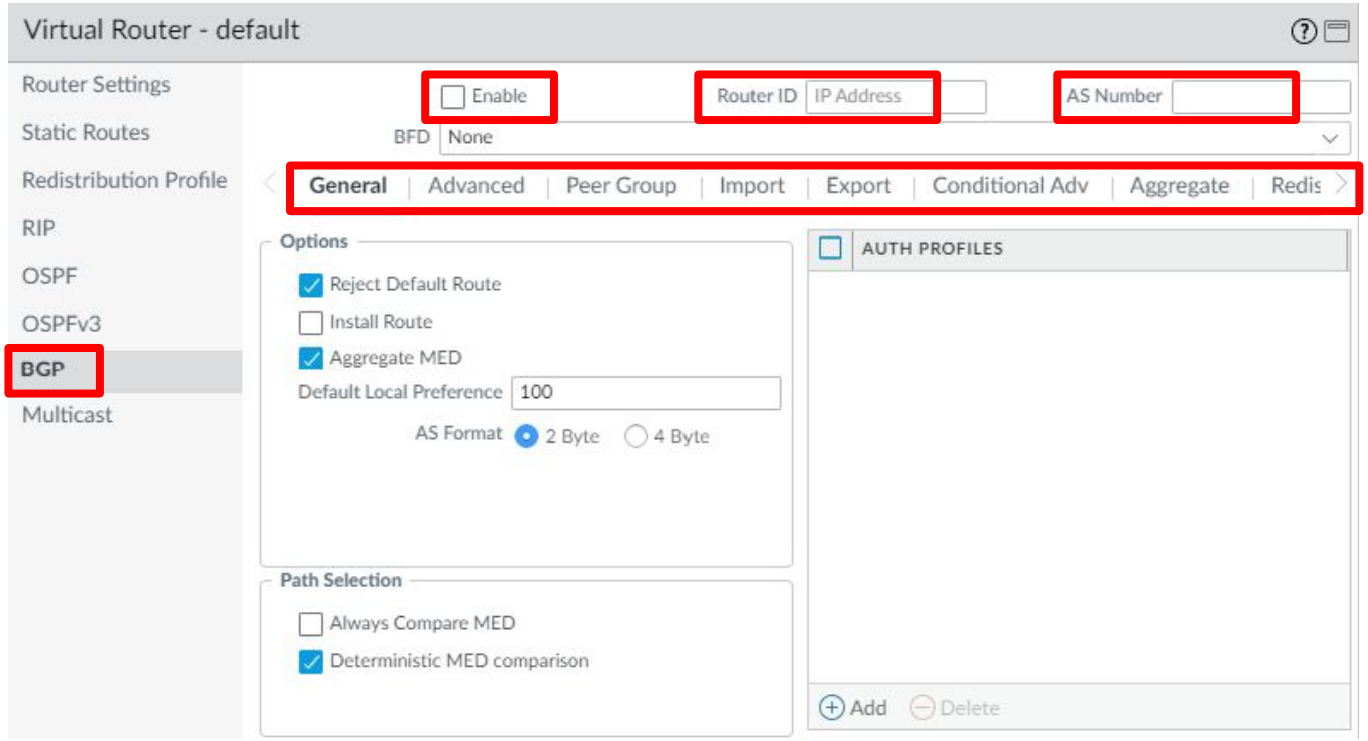
Routing

OSPF:



Routing

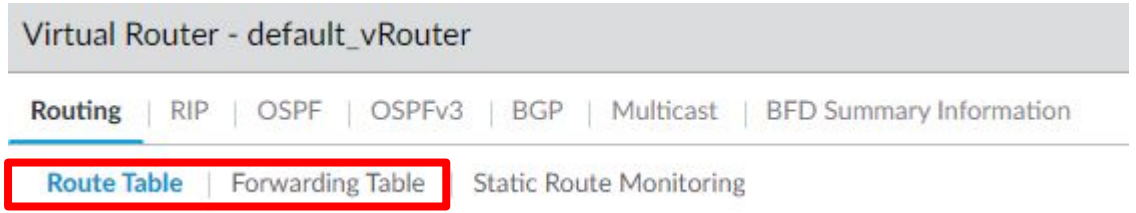
BGP:



Routing

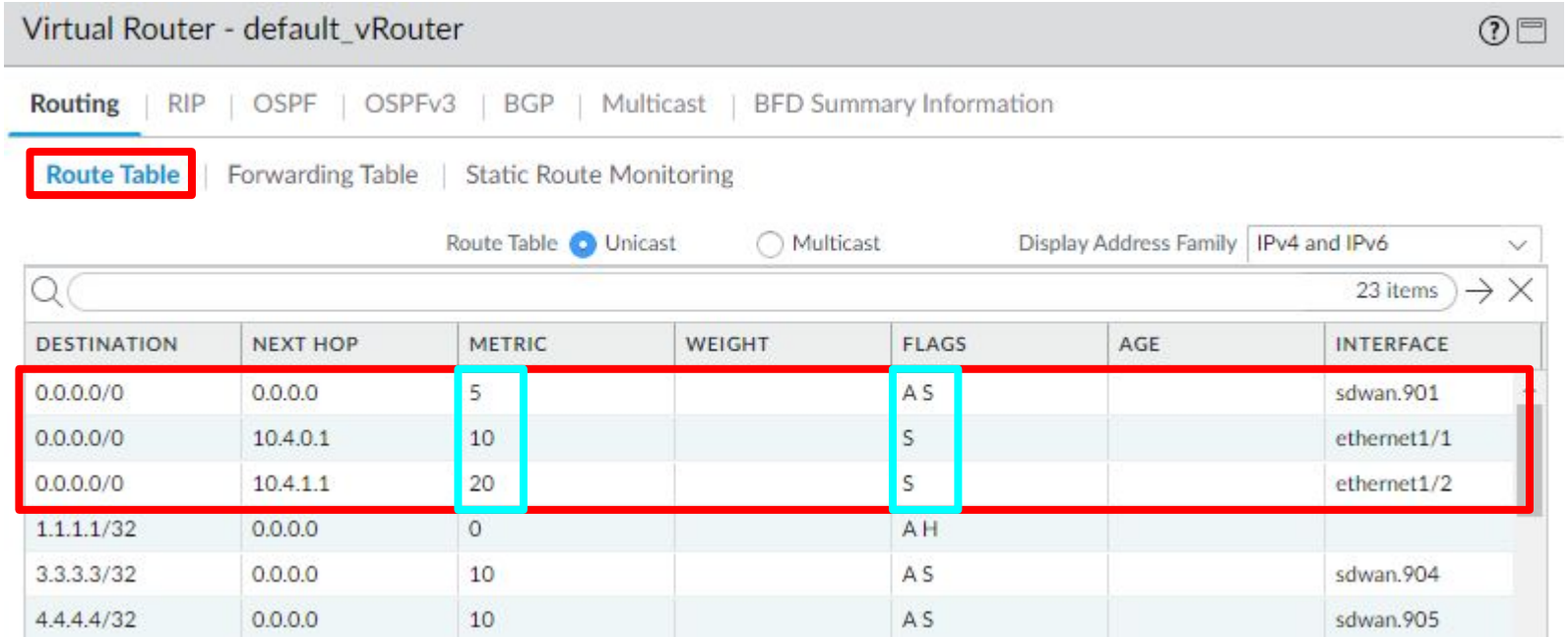
Routing databases:

- Route Table (RIB) - Where all routes are stored
- Forwarding Table (FIB) - Where the route used to forward traffic is stored



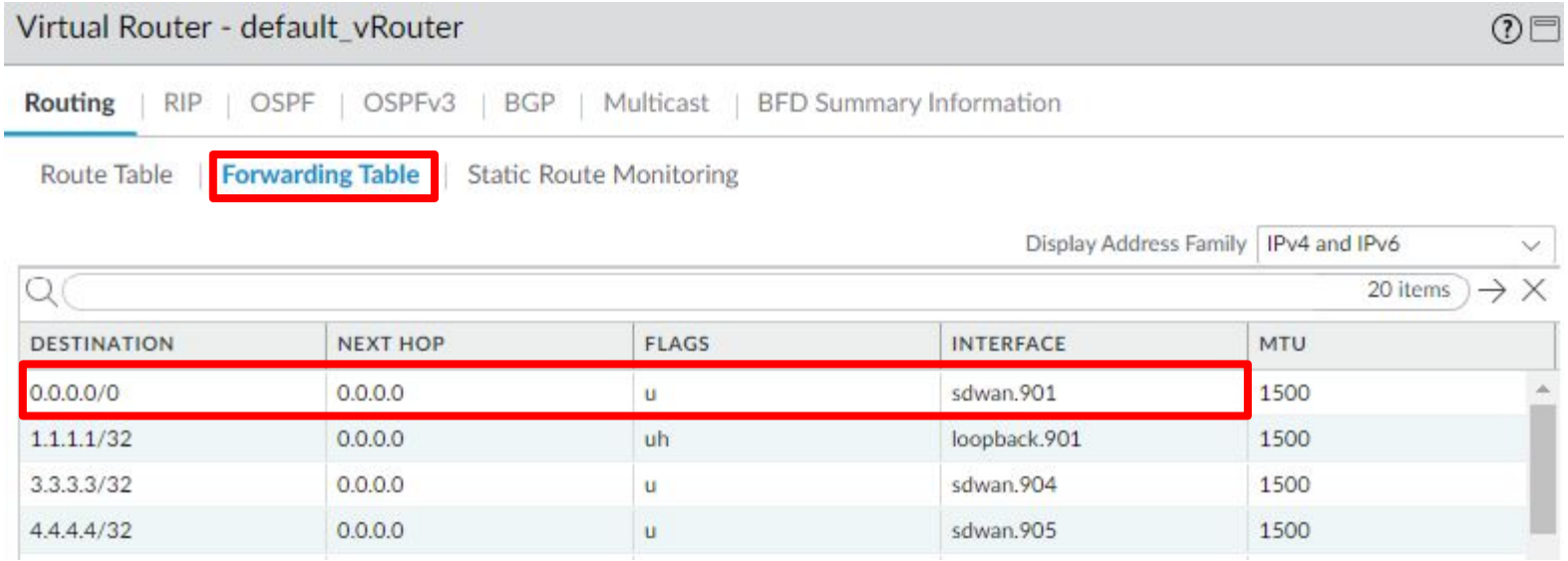
Routing

Routing databases:



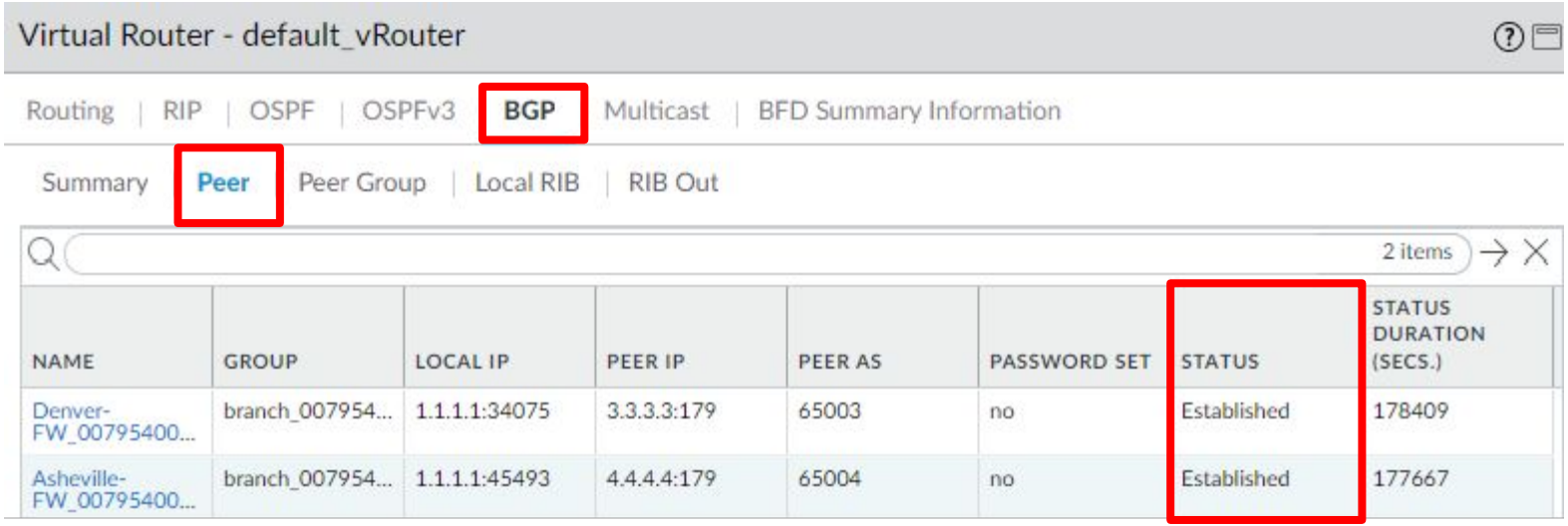
Routing

Routing databases:



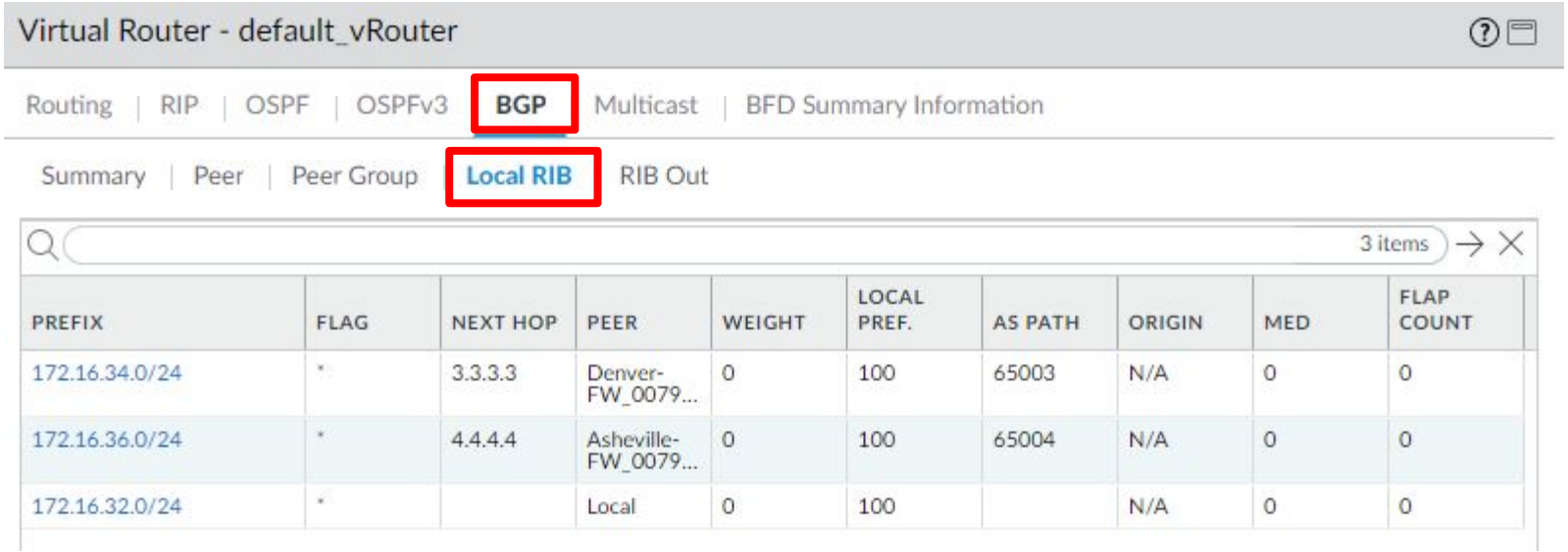
Routing

Routing databases: BGP



Routing

Routing databases: BGP

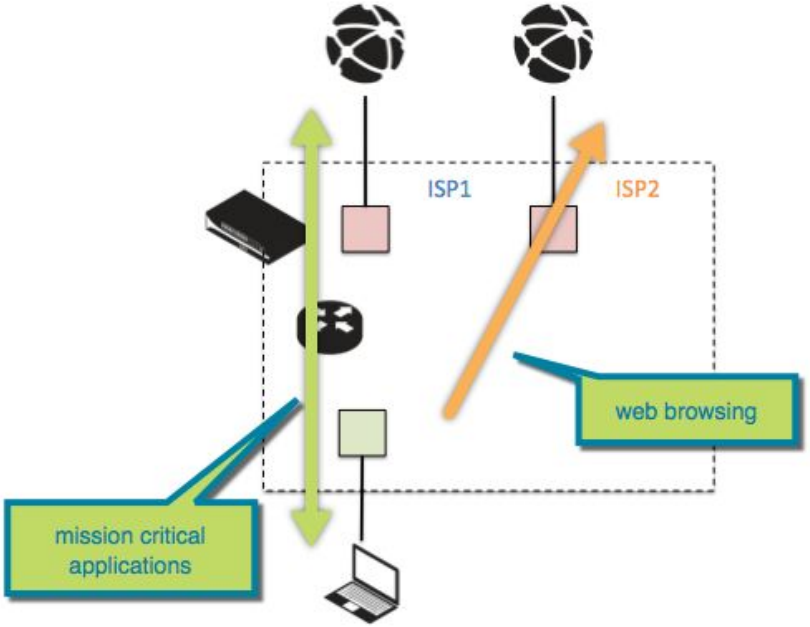


PREFIX	FLAG	NEXT HOP	PEER	WEIGHT	LOCAL PREF.	AS PATH	ORIGIN	MED	FLAP COUNT
172.16.34.0/24	*	3.3.3.3	Denver-FW_0079...	0	100	65003	N/A	0	0
172.16.36.0/24	*	4.4.4.4	Asheville-FW_0079...	0	100	65004	N/A	0	0
172.16.32.0/24	*		Local	0	100		N/A	0	0

Policy Based Forwarding

Policy Based Forwarding

Policy Based Routing: KB Link



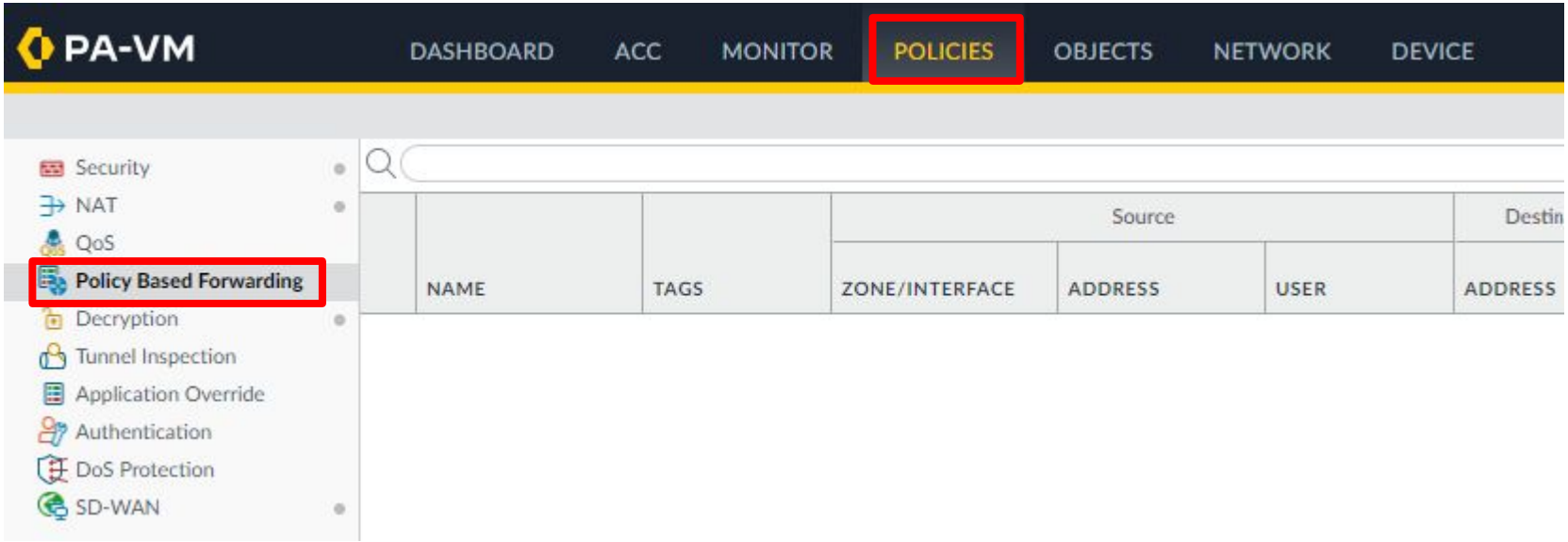
Policy Based Forwarding

Policy Based Routing: KB Link

- Create Static Routes to each ISP and set the metric of the primary lower than the secondary
- Create a Policy Based Forwarding Policy
- Create Security Policy
- Create NAT Policies

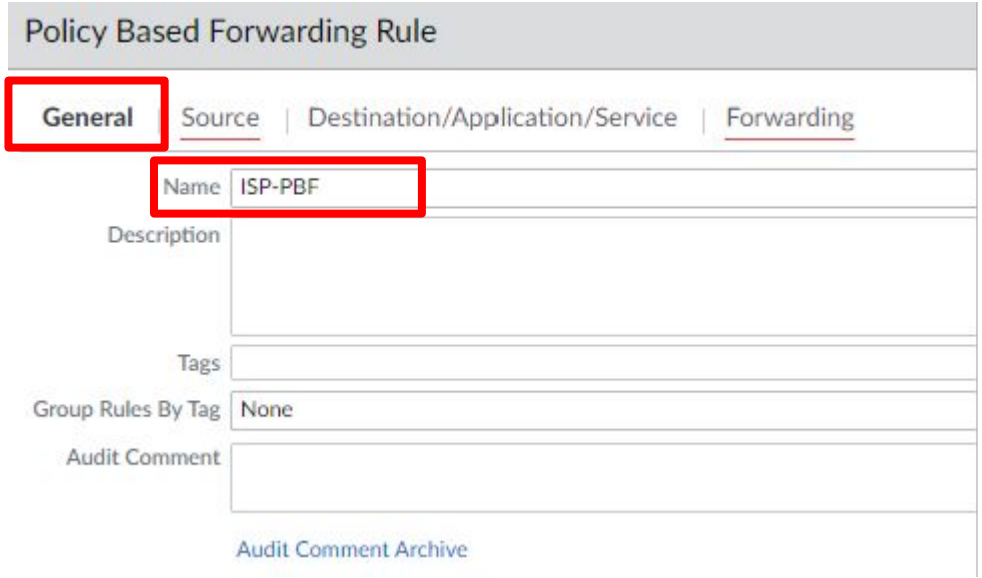
Policy Based Forwarding

Policy Based Routing: KB Link



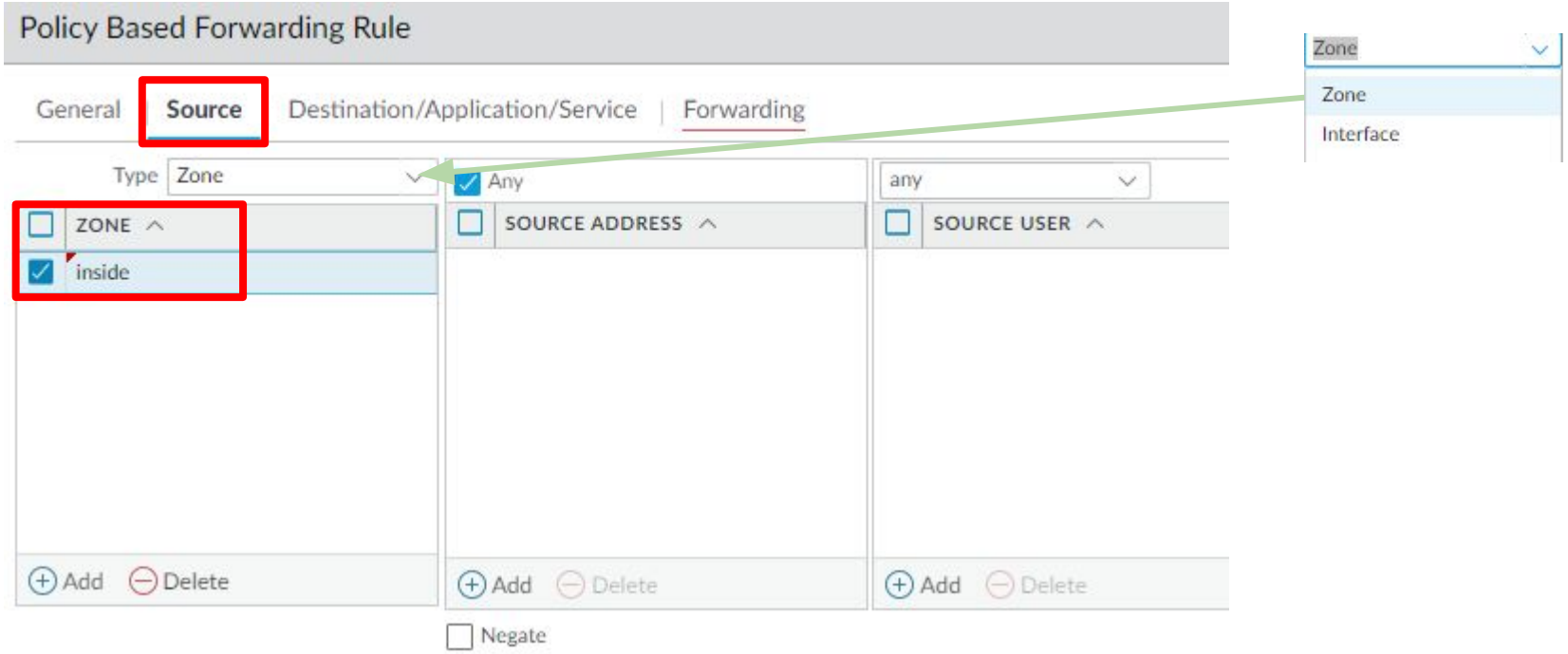
Policy Based Forwarding

Policy Based Routing: KB Link



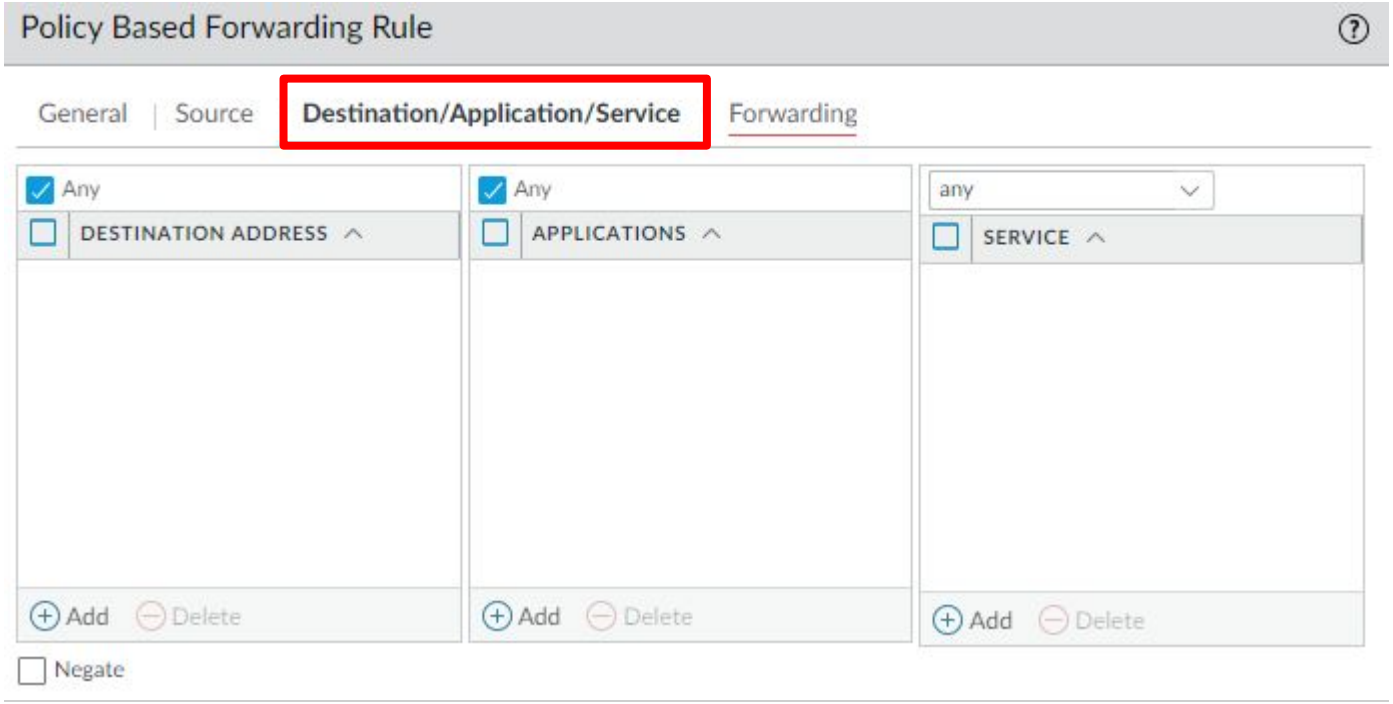
Policy Based Forwarding

Policy Based Routing: KB Link



Policy Based Forwarding

Policy Based Routing: KB Link



Policy Based Forwarding

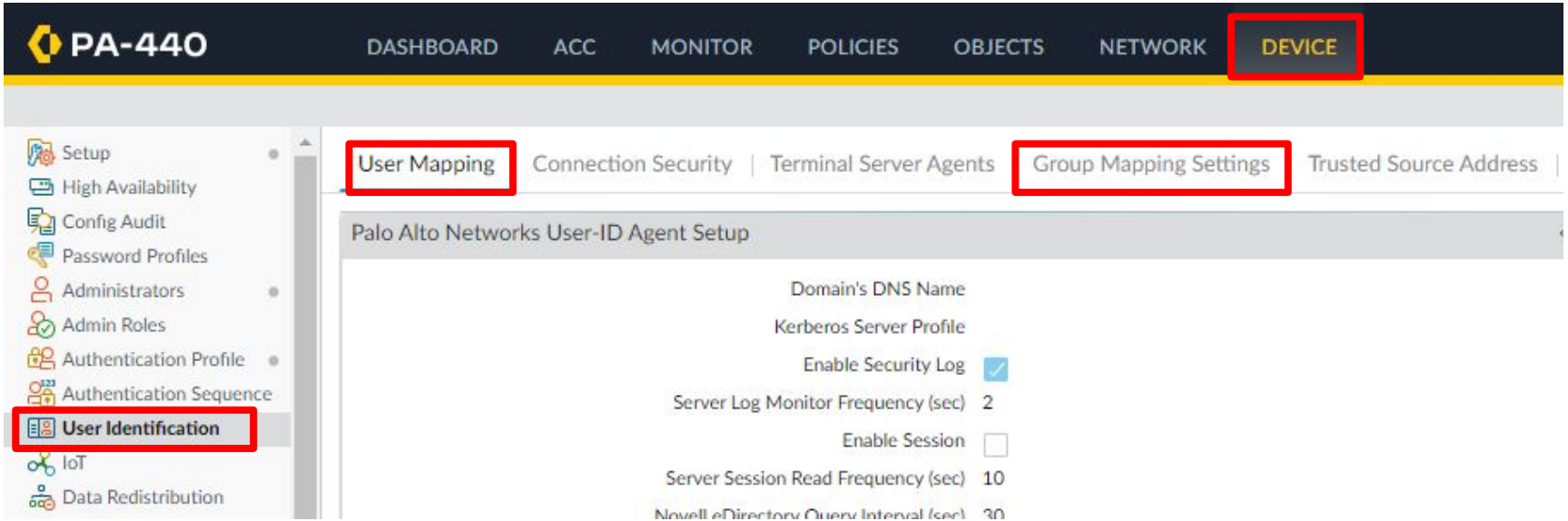
Policy Based Routing: KB Link

USER-ID

USER-ID

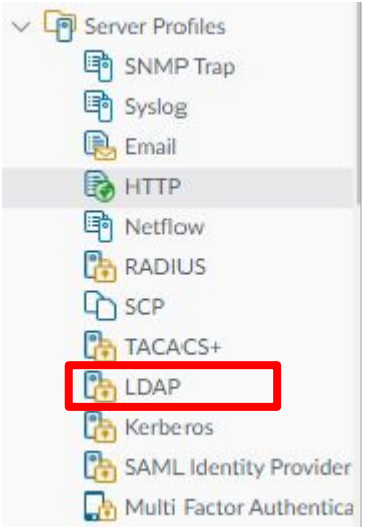
USER-ID Concepts:

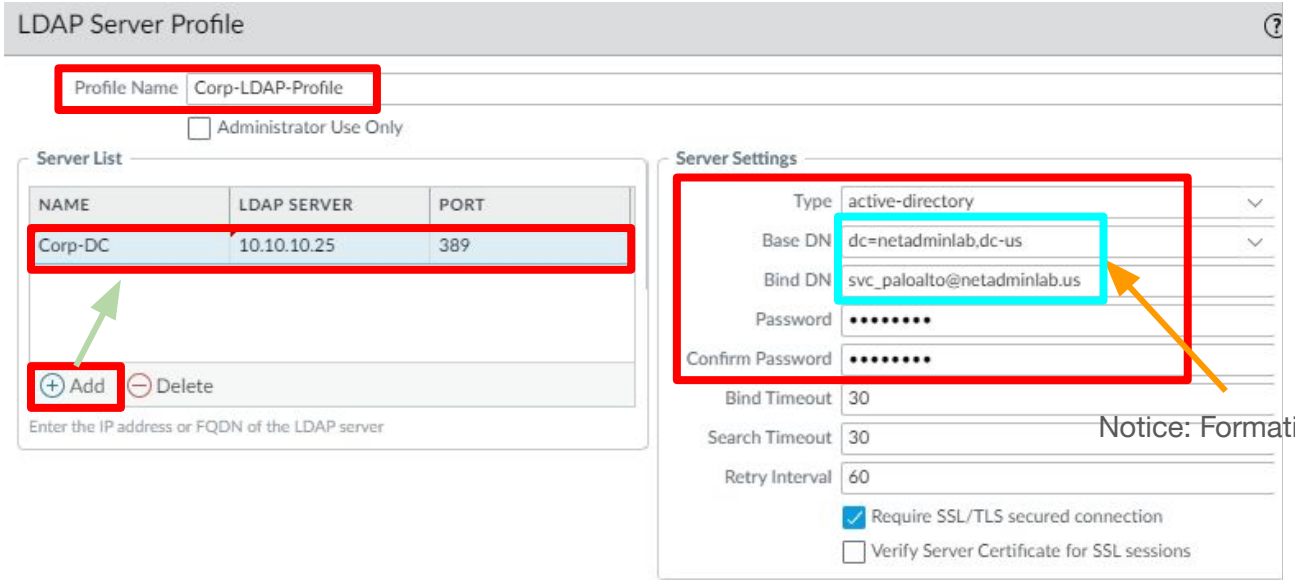
- Group Mapping - User to Group
- User Mapping - User to IP



USER-ID

Server Profile:

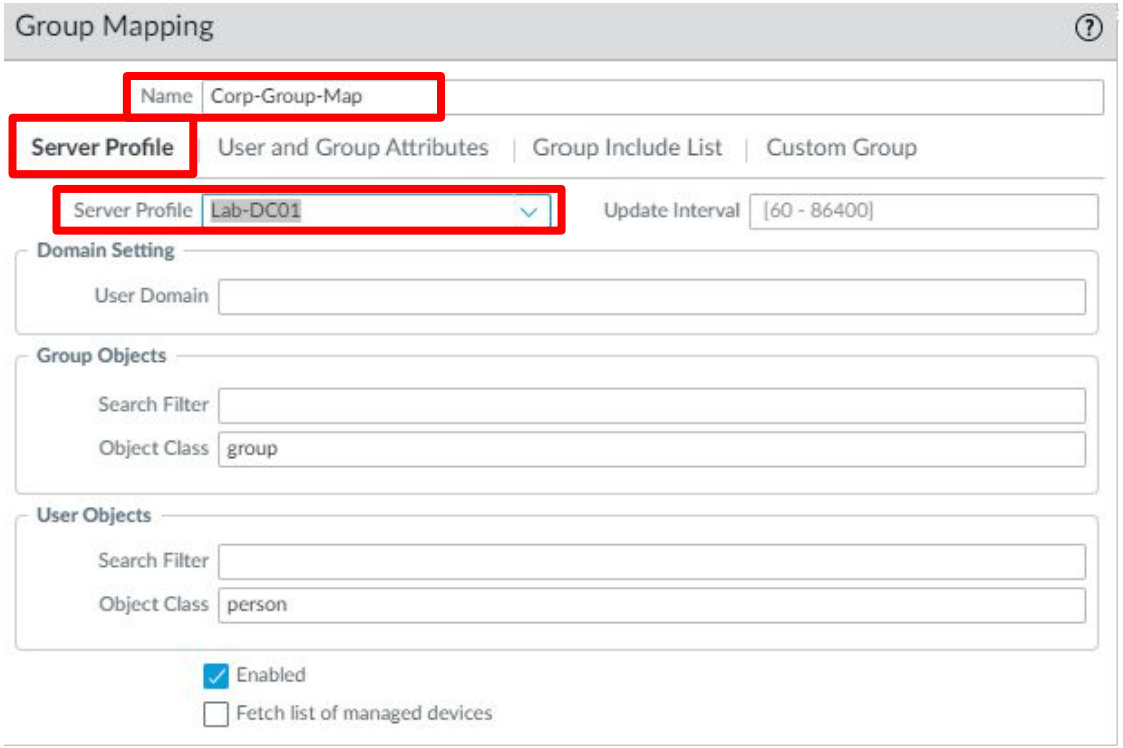


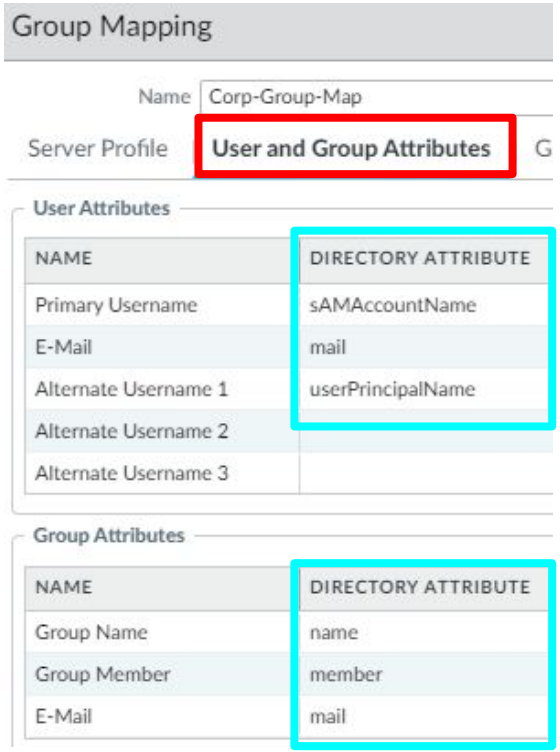


Notice: Formating

USER-ID

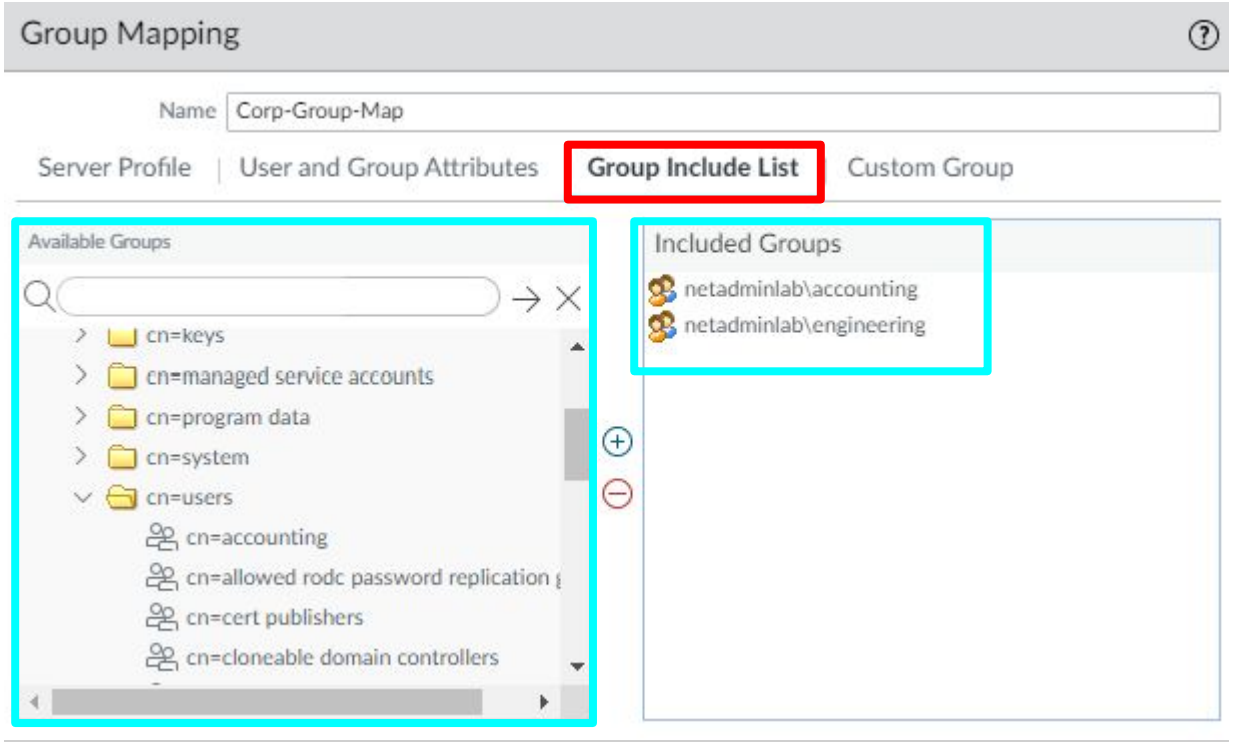
Group Mapping:





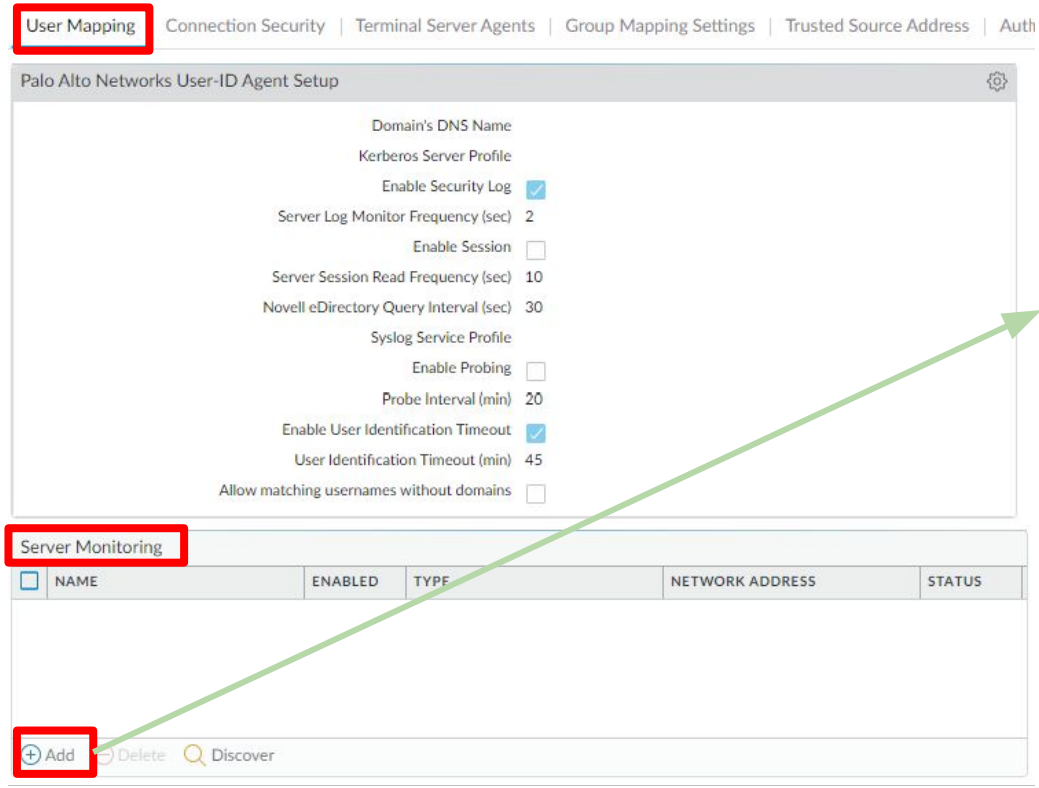
USER-ID

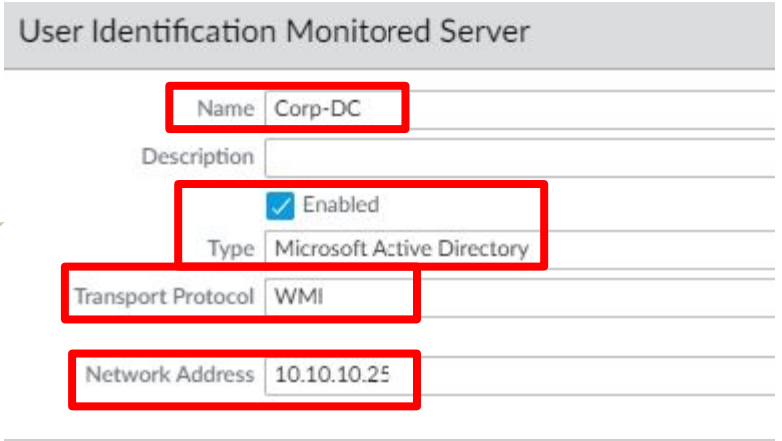
Group Mapping:



USER-ID

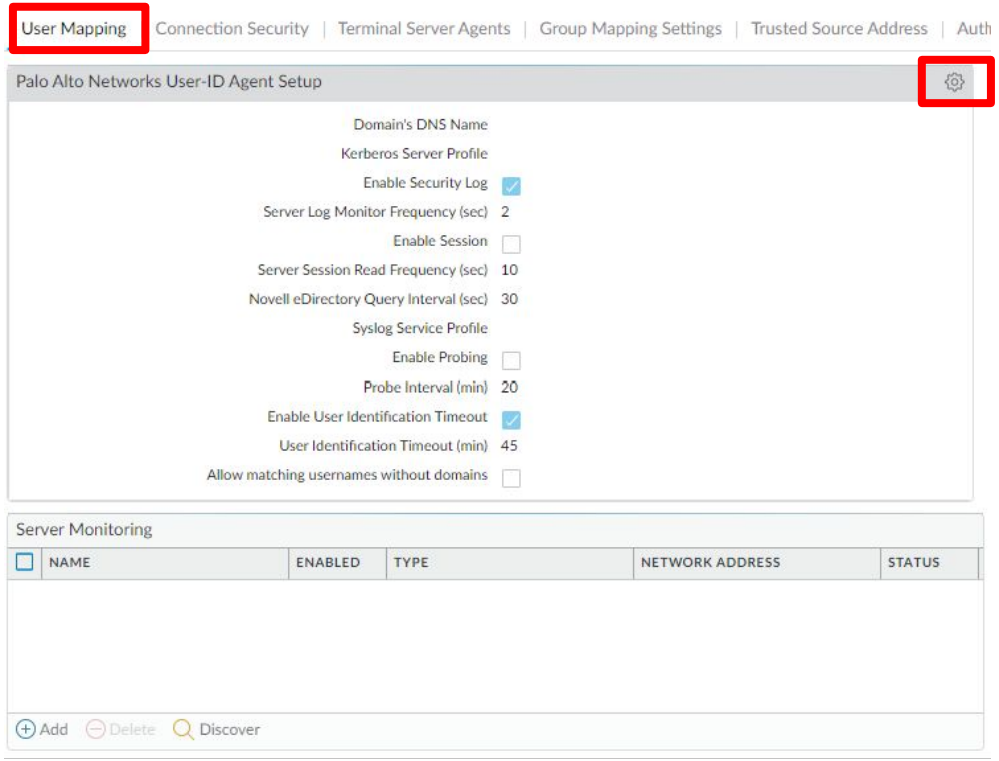
User Mapping: PAN-OS Integrated Agent (Document)





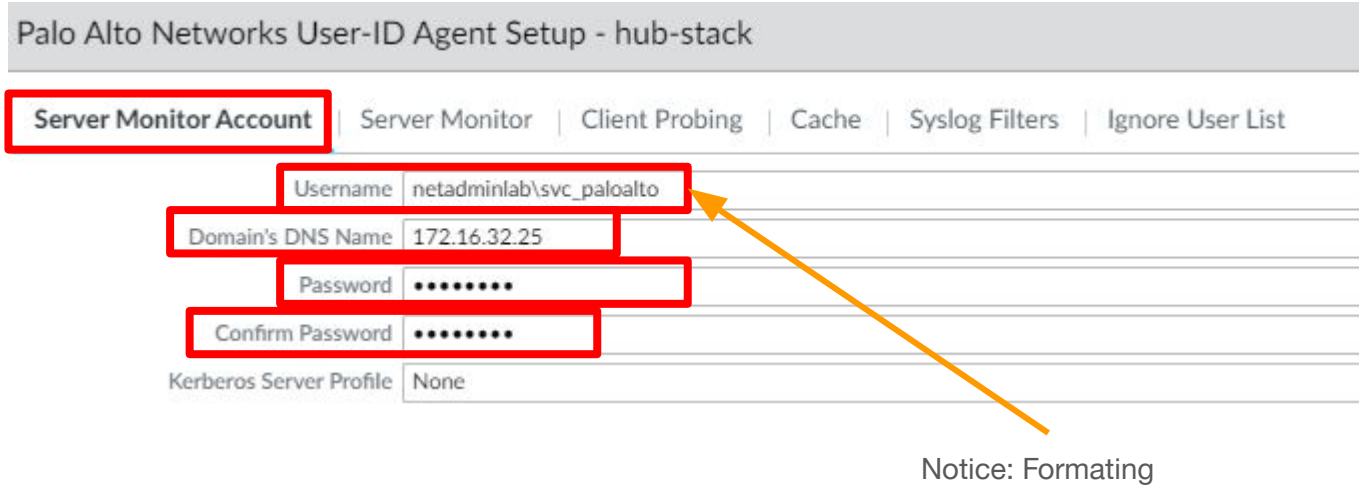
USER-ID

User Mapping: PAN-OS Integrated Agent



USER-ID

User Mapping: PAN-OS Integrated Agent



USER-ID

User Mapping: Windows Agent (Document)

- Install Windows Based User Agent (Document)
  - Install on a domain server
- Configure Windows Based Agent (Document)

User Mapping: Terminal Server Users

- Map individual users coming from a TS environment
- Supported TS
  - Windows
  - Citrix

Troubleshooting

Troubleshooting

Configuration Vs Break fix issues: Support Datasheet

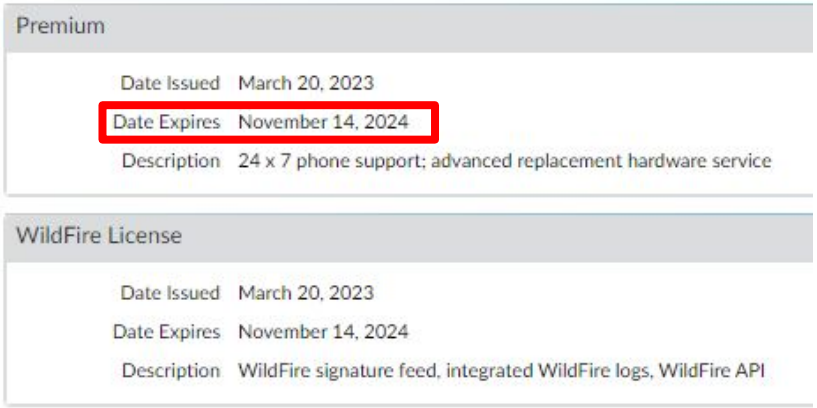
- Palo Alto Support is a break fix organization.
- Palo Alto Partners are used for configuration support.

- New configurations not working are not break fix issues. Putting in a ticket for these types of issues will not get you a resolution.
- Break fix is based on previously functioning configuration or device that has stopped working. This could be due to a software upgrade, content update, bug, device failure, etc.

Troubleshooting

Management: License and Content/PANOS download issues

- Does the device have access to the internet?
- Is the device able to resolve DNS?
- Is the management interface the path to the internet?
- Did you activate the licenses or apply the authorization code?
- Do you own the license for the feature you are trying to use?
- Do you have support on the device?



Troubleshooting

Troubleshooting tool:

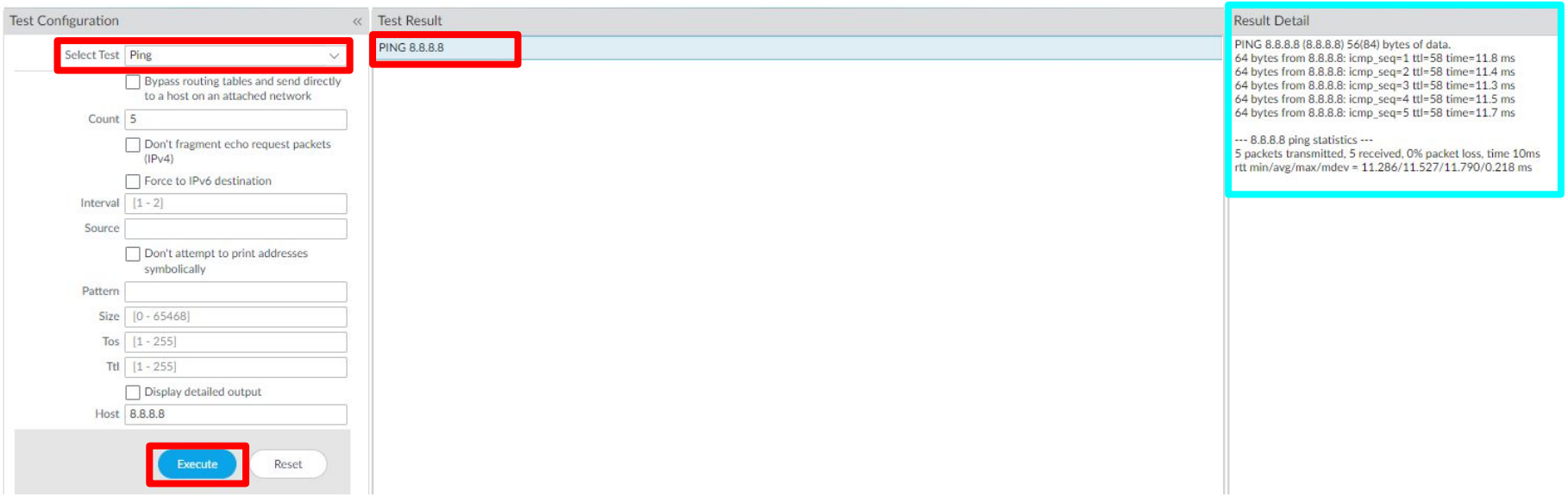
Device -> Troubleshooting

- Policy Match Tests
  - Security Policy Match
  - QoS Policy Match
  - Authentication Policy Match
  - Decryption/SSL Policy Match
  - NAT Policy Match
  - Policy Based Forwarding Policy Match
  - DoS Policy Match

- Connectivity Tests
  - Routing
  - Ping
  - Trace Route
  - Log Collector Connectivity
  - External Dynamic List
  - Test Cloud Logging Service Status
  - Test Cloud GP Service Status
  - Test Wildfire
  - Threat Vault
  - Update Server

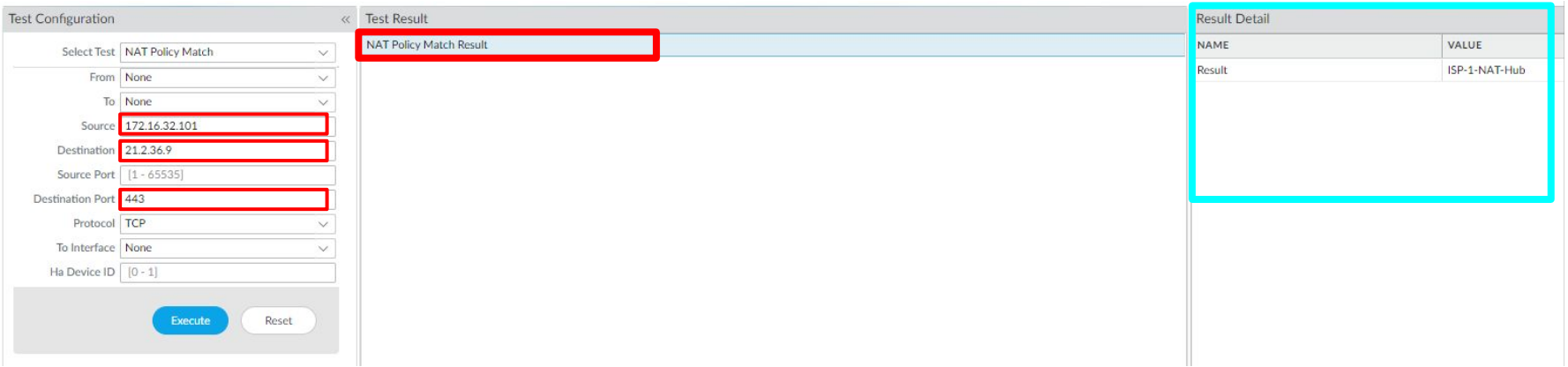
Troubleshooting

Ping:



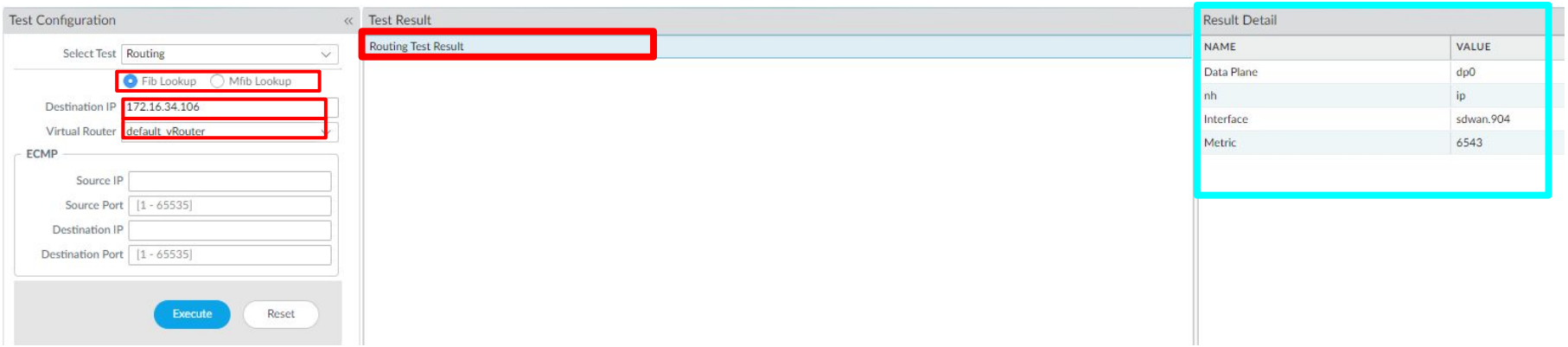
Troubleshooting

NAT Policy Match:



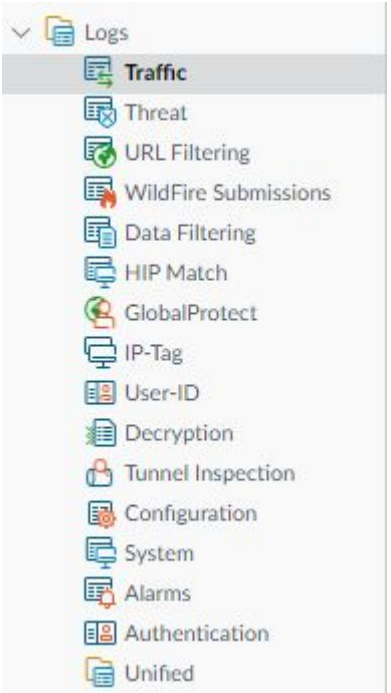
Troubleshooting

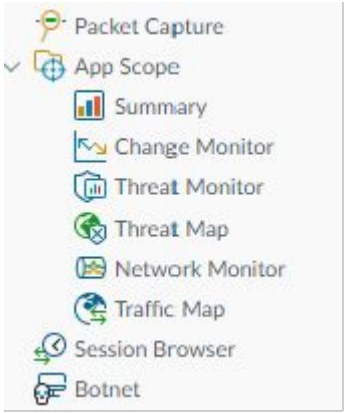
Routing Test:



Troubleshooting

Monitor:





Troubleshooting

Monitor: Traffic Logs

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT DEST IP	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE
		03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.1.2	172.217.215.100	netadminlab\sue		172.217.215.100			443	ssl	allow	Allow-Files-MSUpdate
		03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.0.2	172.217.215.100	netadminlab\sue		172.217.215.100			443	ssl	allow	Allow-Files-MSUpdate
		03/01 09:22:53	end	inside	outside	172.16.32.25	10.4.0.2	208.67.222.222			208.67.222.222			53	dns-base	allow	Inside-to-Outside-Traffic
		03/01 09:22:53	end	inside	outside	172.16.32.25	10.4.1.2	208.67.222.222			208.67.222.222			53	dns-base	allow	Inside-to-Outside-Traffic
		03/01 09:22:53	end	inside	outside	172.16.32.101	10.4.1.2	74.125.136.190	netadminlab\sue		74.125.136.190			443	youtube-base	allow	Inside-to-Outside-Traffic

Detailed Log View

General

Session ID	97955
Action	allow
Action Source	from-policy
Host ID	
Application	ssl
Rule	Allow-Files-MSUpdate
Rule UUID	acad8078-2f1b-425d-b92e-d89cedb437ed
Session End Reason	tcp-fin

Source

Source User	netadminlab\sue
Source	172.16.32.101
Source DAG	
Country	172.16.0.0-172.31.255.255
Port	63541
Zone	inside
Interface	ethernet1/3
NAT IP	10.4.1.2
NAT Port	13375

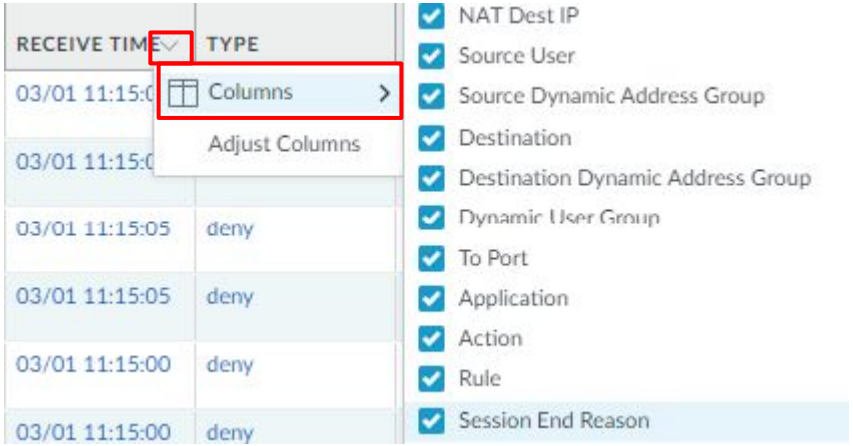
Destination

Destination User	
Destination	172.217.215.100
Destination DAG	
Country	United States
Port	443
Zone	outside
Interface	sdwan.901
NAT IP	172.217.215.100
NAT Port	443

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2024/03/01 09:22:53	end	ssl	allow	Allow-Files-MSUp...	acad80...	17...		any				

Troubleshooting

Changing views for information gathering.



Troubleshooting

Filtering Logs:

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT DEST IP	SOURCE USER
		03/01 11:15:05	deny	zone-to-branch	inside	172.16.34.1			netadminlab\svc...
		03/01 11:15:05	deny	zone-to-branch	inside	172.16.36.1			netadminlab\svc...
		03/01 11:15:05	deny	zone-to-branch	inside	172.16.34.1			netadminlab\svc...

Click to add as a filter

Troubleshooting

Monitor: Traffic Log: NAT Translations

FROM ZONE	TO ZONE	SOURCE	NAT SOURCE IP	NAT SOURCE PORT	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION
lan_zone	wan_zone	192.168.18.100	173.235.189.251	0			134.238.183.164
lan_zone	wan_zone	10.0.41.102	173.235.189.251	6890			17.253.7.141
lan_zone	wan_zone	192.168.18.100	173.235.189.251	7598			170.114.52.2
lan_zone	wan_zone	192.168.18.100	173.235.189.251	14309			17.253.97.203
lan_zone	wan_zone	10.0.40.106	173.235.189.251	52330			71.18.43.229
lan_zone	lan_zone	192.168.18.100		0			192.168.18.1
lan_zone	wan_zone	10.0.40.109	173.235.189.251	28849			8.8.8.8
wan_zone	wan_zone	65.49.20.73		0			173.235.189.251

Troubleshooting

Monitor: Threat Logs

		RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	SEVERITY
		12/20 15:14:54	spyware	Parked:gixel.gnetwork.me	inside	outside	172.16.32.25			208.67.222.222			53	dns-base	alert	informational
		04/28 13:38:30	flood	PBP Packet Drop	outside		10.6.0.2			0.0.0.0			0	not-applicable	drop	high
		04/27 10:43:23	flood	PBP Packet Drop	outside		10.4.0.2			10.5.1.2			27407	not-applicable	drop	high
		04/27 10:42:19	flood	PBP Packet Drop	outside		10.4.1.2			10.5.0.2			17876	not-applicable	drop	high

Troubleshooting

Monitor: URL Logs

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS INSERTED	HTTP/2 CONNECTION SESSION ID
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:32:49	computer-and-internet-info	computer-and-internet-info,low-risk	v10.vortex-win.d...	inside	outside	172.16.32.25			51.132.193.104			ssl	alert		0
	03/01 09:25:29	streaming-media	streaming-media,low-risk	www.youtube.c...	inside	outside	172.16.32.101	netadminlab\sue		142.250.105.91			youtube-base	alert		98632
	03/01 09:24:58	web-advertisements	web-advertisements,low risk	match.adsrvr.org...	inside	outside	172.16.32.101	netadminlab\sue		3.33.220.150			web-browsing	alert		98716

Troubleshooting

Monitor: Configuration

RECEIVE TIME	ADMINISTRAT...	HOST	CLIENT	COMMA...	RESULT	CONFIGURATION PATH	FULL PATH	BEFORE CHANGE	AFTER CHANGE	SEQUENCE NUMBER
02/29 14:01:08	admin	192.168.18.100	Web	commit	Submitted					7333601583554363397
02/29 14:01:02	admin	192.168.18.100	Web	delete	Succeed...	vsys vsys1 external-list CINS Army Feed	/config/devices/... list/entry[@nam... Army Feed']			7333601583554363396
02/29 14:00:43	admin	192.168.18.100	Web	delete	Succeed...	vsys vsys1 rulebase security rules Test EDL	/config/devices/... EDL']	43decde9-12f9-412c-ab9f-32019a4f27a4		7333601583554363395
02/29 13:55:53	admin	192.168.18.100	Web	commit	Submitted					7333601583554363394
02/29 13:55:44	admin	192.168.18.100	Web	set	Succeed...	vsys vsys1 rulebase security rules Test EDL	/config/devices/... EDL']		Test EDL 43decde9-12f9-412c-ab9f-32019a4f27a4 { profile-setting	7333601583554363393
02/29 13:54:09	admin	192.168.18.100	Web	set	Succeed...	vsys vsys1 external-list CINS Army Feed	/config/devices/... list/entry[@nam... Army Feed']		external-list { CINS Army Feed { type { ip { recurring { five-m	7333601583554363392
01/05 16:57:23	Panorama-admin	0.0.0.0	Panorama	commit-all	Submitted					7320737447833239553

Troubleshooting

Monitor: Unified

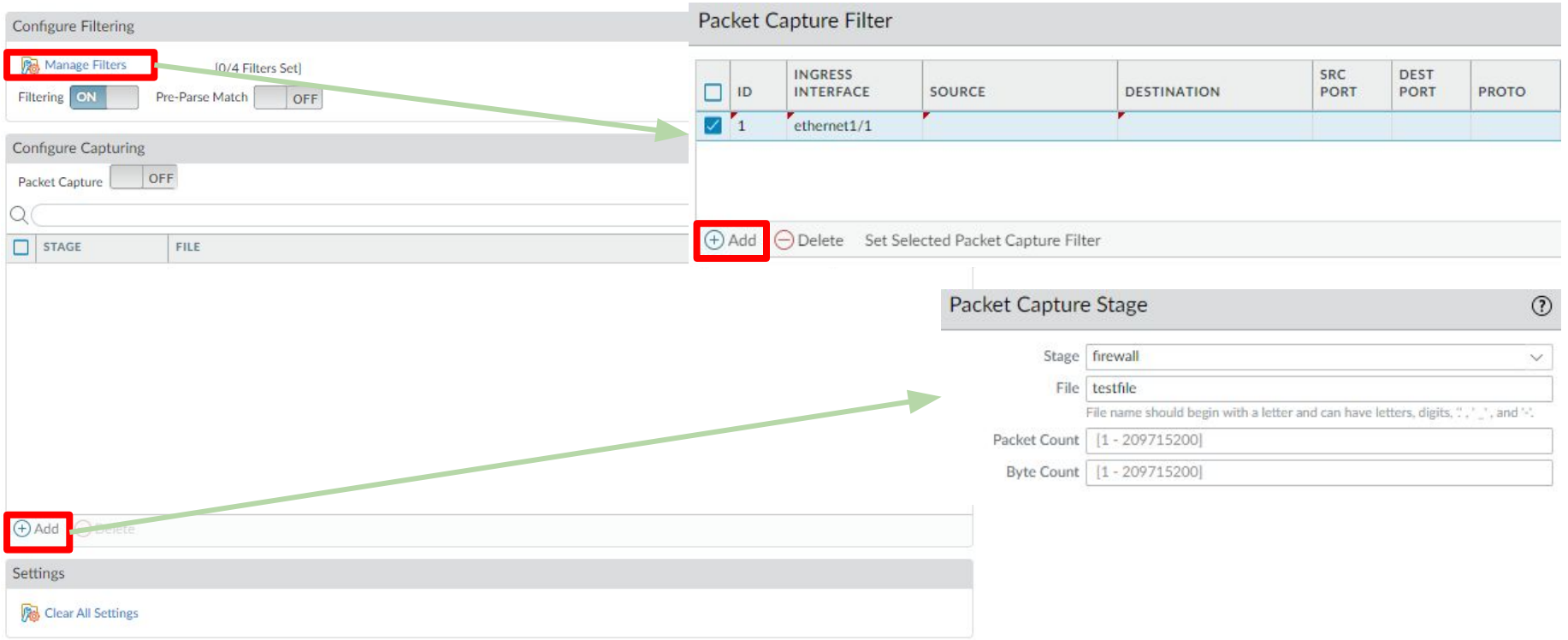
	LOG TYPE	RECEIVE TIME	LOG SUBTYPE	SESSION ID	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DEST... PORT	DESTINATION DYNAMIC ADDRESS GROUP	APPLICATION	ACTION	RULE	BYTES	THREAT ID/NAME	SEVERITY
	url	03/01 09:32:49	url	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	alert	Allow-Files-MSUpdate			Informational
	decryption	03/01 09:32:44	0	98962	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate			
	decryption	03/01 09:32:44	0	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate			
	decryption	03/01 09:32:44	0	98953	inside	outside	172.16.32.25			52.167.17.97	443		incomplete	allow	Allow-Files-MSUpdate			
	traffic	03/01 09:32:44	deny	98962	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate	304		
	traffic	03/01 09:32:44	deny	98950	inside	outside	172.16.32.25			51.132.193.104	443		ssl	allow	Allow-Files-MSUpdate	5.2k		

LOG TYPE
url
decryption
decryption
decryption
traffic
traffic

Multiple logs consolidated into one location

Troubleshooting

Device -> Packet Capture



Troubleshooting

Monitor: Session Browser

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATION	FROM PORT	TO PORT	PROTOCOL	APPLICATION	RULE	INGRESS I/F	EGRESS I/F	BYTES
02/29 22:38:20	lan_zone	wan_zone	192.168.18.42	34.111.222.75	34904	443	6	paloalto-dlp-service	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	510634
03/01 11:12:00	lan_zone	wan_zone	10.0.40.109	8.8.8.8	44421	53	17	dns-base	LAN-to-WAN-Traffic	ethernet1/1.400	ethernet1/2	188
03/01 11:11:51	lan_zone	wan_zone	192.168.18.33	8.8.8.8	44251	53	17	dns-base	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	303
02/29 11:16:39	lan_zone	wan_zone	192.168.18.100	52.159.127.243	49424	443	6	windows-push-notifications	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	76156
03/01 11:11:45	lan_zone	wan_zone	192.168.18.30	192.0.2.2	44906	514	17	syslog	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	1363
03/01 11:12:07	lan_zone	wan_zone	192.168.18.42	35.184.126.116	33298	443	6	paloalto-device-telemetry	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	31294
03/01 11:09:52	lan_zone	wan_zone	192.168.18.13	107.178.249.217	37787	443	6	paloalto-updates	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	17960
03/01 11:03:09	lan_zone	wan_zone	192.168.18.50	34.235.175.181	37572	443	6	ssl	LAN-to-WAN-Traffic	ethernet1/1	ethernet1/2	66513
03/01 11:11:49	lan_zone	wan_zone	10.0.40.106	104.84.231.148	60052	443	6	tiktok-base	LAN-to-WAN-Traffic	ethernet1/1.400	ethernet1/2	519372

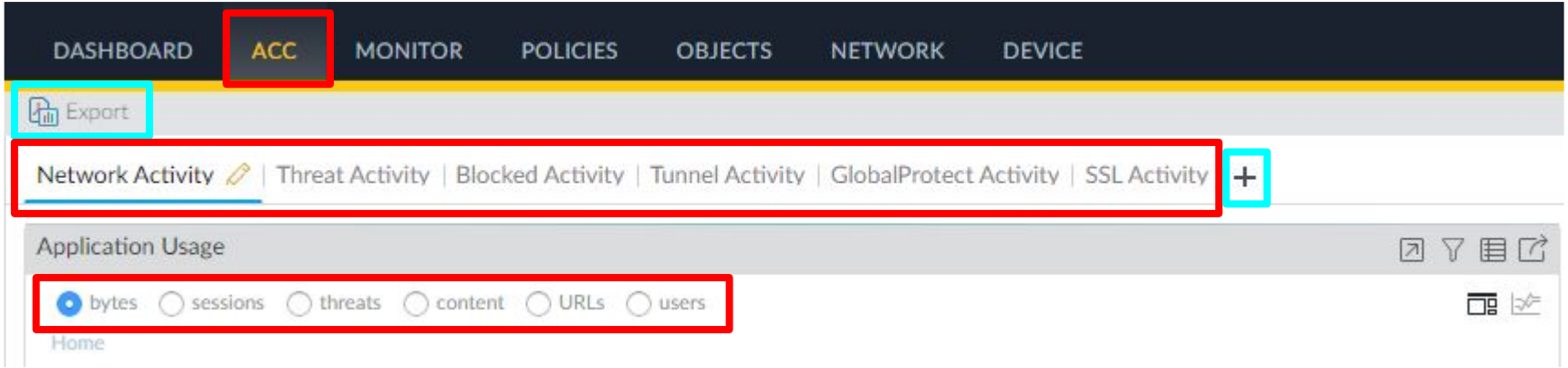
Troubleshooting

Command Line Interface: Cheat Sheet

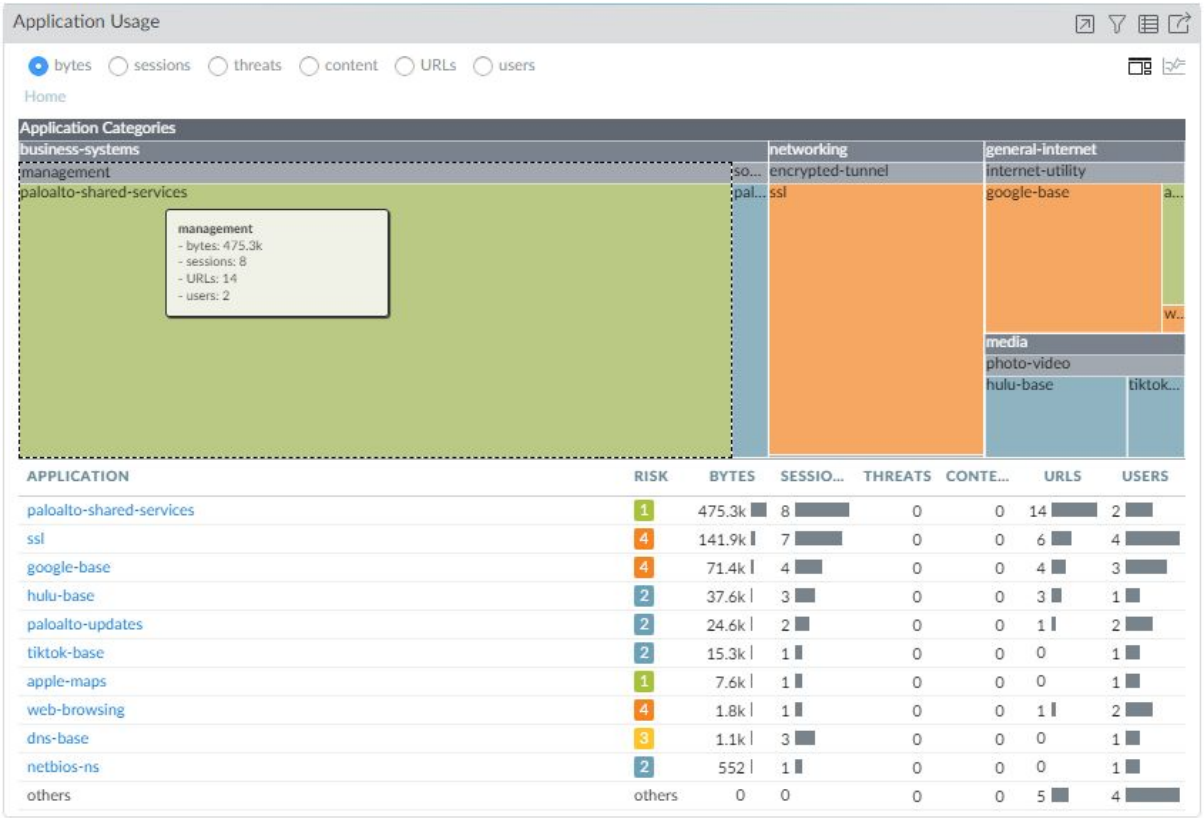
- show system info
- show system resources
- show running resource-monitor
- request restart system
- show user group-mapping statistics
- show user group-mapping state all
- show user group list
- show user group name <group-name>
- show user ip-user-mapping all
- show routing route
- ping host <destination-ip-address>
- ping source <ip-address-on-dataplane> host <destination-ip-address>

Troubleshooting

Application Control Center (ACC):



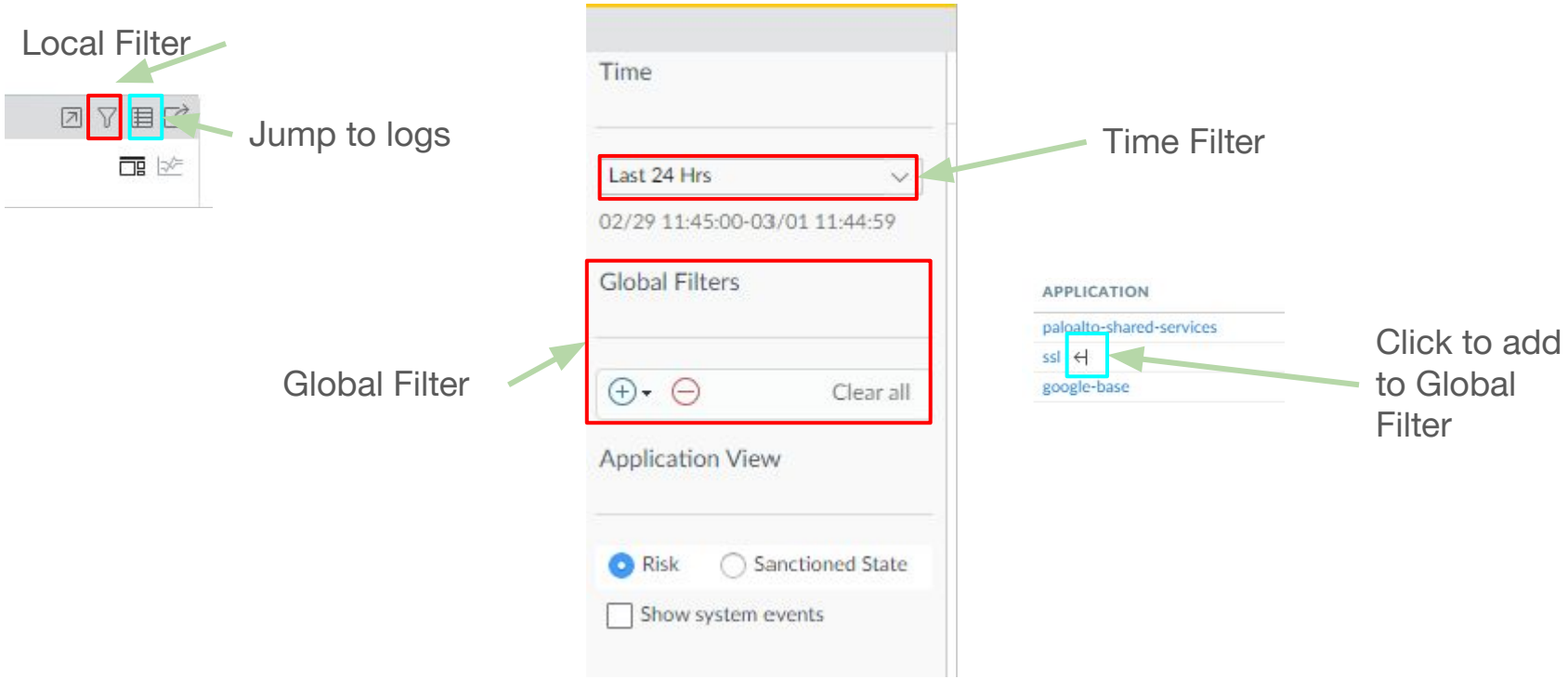
Troubleshooting



APPLICATION	RISK	BYTES	SESSIO...	THREATS	CONTE...	URLS	USERS
paloalto-shared-services	1	475.3k	8	0	0	14	2
ssl	4	141.9k	7	0	0	6	4
google-base	4	71.4k	4	0	0	4	3
hulu-base	2	37.6k	3	0	0	3	1
paloalto-updates	2	24.6k	2	0	0	1	2
tiktok-base	2	15.3k	1	0	0	0	1
apple-maps	1	7.6k	1	0	0	0	1
web-browsing	4	1.8k	1	0	0	1	2
dns-base	3	1.1k	3	0	0	0	1
netbios-ns	2	552	1	0	0	0	1
others	others	0	0	0	0	5	4

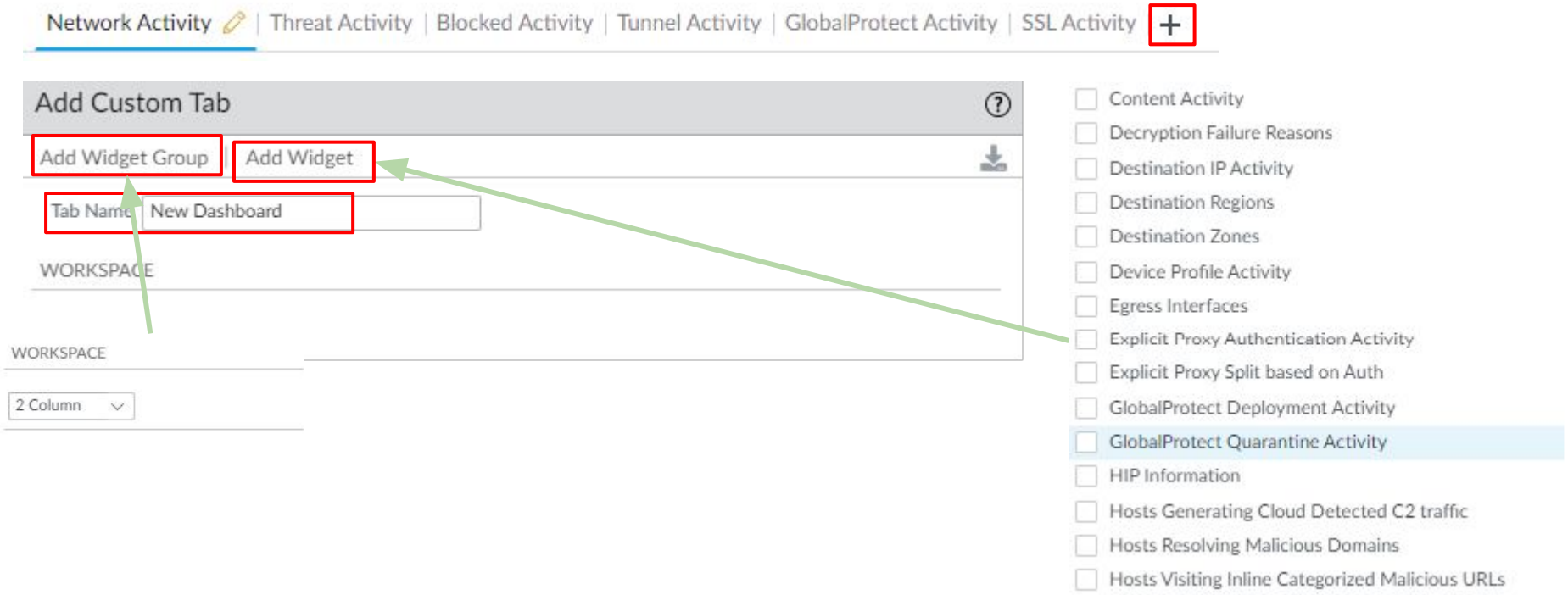
Troubleshooting

ACC: Filtering



Troubleshooting

Creating a new dashboard in the ACC:



Resources

Resources

- PANOS Administrator Guide
- CLI Cheat Sheet
- PANOS Recommended Releases
- Security Advisories
- Applipedia
- Hardware EoL List
- Software EoL List
- Compatibility Matrix
- SCM Pro vs Essentials
- Quick Starts and Hardware Reference
- Product Selector (Specifications)
- PA Series Hardware Architectures

Resources

Purchasing Lab Equipment:

- Palo Alto sells equipment and software designated for testing/lab purposes. This equipment is less expensive than normal equipment with the same functionality. It is not for production as it has a different level of support.
- All customers should have a lab or mock setup for testing purposes. New configurations and software updates should never be introduced into production.
- This is a perfect way to learn and train on platforms without disruptions to your production environment.

Note: for Palo Alto Partners, this equipment is called NFR and not Lab.

Resources

Strata Logging Service (SLS)

Storing firewall logs in SLS provides AI/ML driven analytics to be used in AIOps vs only telemetry data to provide insights into your device health and security posture.

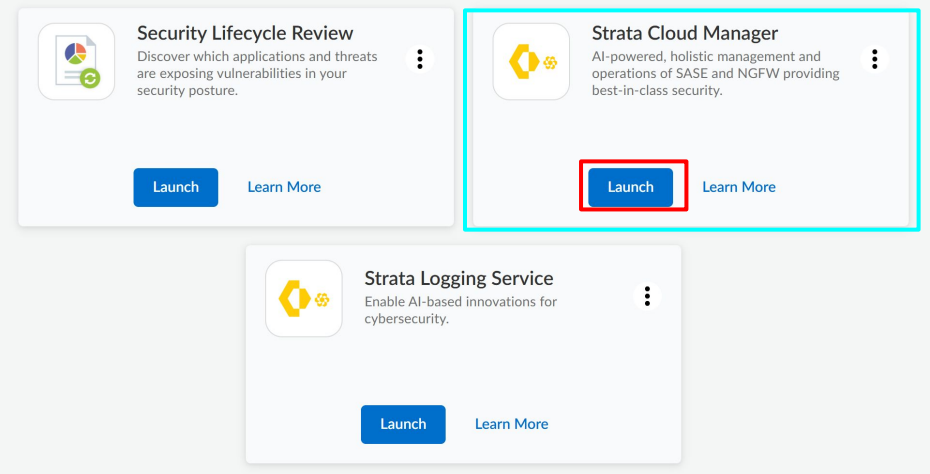
Storing firewall logs in SLS gives you an offsite repository of logs that can be accessed anywhere from the SLS Web App or Panorama.

Off site log storage allows multiple dispersed sites to log to a cloud instance instead of a single Panorama server at one location or multiple log collectors throughout the environment.

Resources

SCM:

- Install a device certificate.
- Setup SLS or Telemetry on NGFW and/or Panorama
- Send information to CDL or Telemetry
- ***** Allow 24 hours between these steps *****
- Activate your AIOps subscription in The Hub



Resources

SCM: Pro Vs Essentials

Strata Cloud Manager Essentials

- Command Center and Activity Insights
- Best Practices Reporting
- Health Insights and Alerts
- Configuration and Policy Management

Strata Logging Service - Optional Add-On (Paid)

Strata Cloud Manager Pro

Command Center and Activity Insights	AI-Powered ADEM
Best Practices Reporting	Real-Time, Inline Best Practices
Health Insights and Alerts	AI-Powered Policy Analysis
Configuration and Policy Management	**AI-Powered Operational Health** *Failure Prediction, Probable Cause Analysis, Capacity Analyzer, Anomaly Detection*
Strata Logging Service *Includes 1 year of retention*	**Software Upgrade Analysis and Recommendations**

Questions?

Thank You!